TAMPEREEN TEKNILLINEN YLIOPISTO

MIKKO SIPILÄ

TIETOSUOJA JA YKSITYISYYS KULUTTAJILLE SUUNNATUISSA PILVIPALVELUISSA

Diplomityö

Tarkastaja: professori Jarmo Harju
Tarkastaja ja aihe hyväksytty Tieto- ja sähkötekniikan tiedekuntaneuvoston kokouksessa 08.05.2013

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Signaalinkäsittelyn ja tietoliikennetekniikan koulutusohjelma
SIPILÄ, MIKKO: Tietosuoja ja yksityisyys kuluttajille suunnatuissa pilvipalveluissa
Diplomityö, 47 sivua
Lokakuu 2013
Pääaine: Tietoliikennetekniikka
Tarkastaja: professori Jarmo Harju
Avainsanat: Tietoturva, Pilvipalvelu, Pilvilaskenta, Tietosuoja, Yksityisyys

Pilvipalveluiden käyttö lisääntyy nopeasti ja yhä useammat sovellukset, jotka ovat perinteisesti olleet työpöytäsovelluksia, ovat siirtyneet pilveen. Sovellusten perässä pilveen siirtyvät myös yritykset sekä oppilaitokset, jotka kasvavissa määrin hylkäävät vanhat perinteiset ohjelmistot ja ottavat pilvipalveluiden hyödyt käyttöönsä. Pilvipalveluiden etuina ovat kustannustehokkuus sekä mahdollisuus käyttää niitä riippumatta paikasta, ajasta tai laitteesta.

Tutkimuksen tarkoituksena on selvittää suosituimpien pilvipalveluiden käytön uhkia käyttäjän yksityisyydelle ja tietosuojalle. Aihe on ajankohtainen sillä lähes päivittäin uutisissa on kerrottu pilvipalveluihin liittyvistä tietoturvaongelmista.

Tutkimuksessa käy ilmi, että suurimmat ja suosituimmat pilvipalvelut ovat kohtuullisen turvallisia käyttää. Isoilla pilvipalveluita tarjoavilla yrityksillä on varaa panostaa datakeskusten turvallisuuteen, tietoturvien ennaltaehkäisemiseen sekä itse palvelun turvallisuuteen. Yksi suurimmista uhista yksityisyydelle ja tietosuojalle on käyttäjä itse, sillä käyttäjä voi jakaa itsestään liikaa tietoa.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Signal Processing and Communications Engineering
SIPILÄ, MIKKO: Data protection and privacy in consumer cloud services
Master of Science Thesis, 47 pages
Major: Communications Engineering
Examiner: Professor Jarmo Harju
Keywords: Cloud computing, Cloud services, Privacy, Data protection

Cloud services re growing rapidly and more and more applications that have traditionally been desktop applications, have been transferred to the cloud. Also companies and educational institutions are moving to cloud and are increasingly rejecting the old traditional software and take benefits of the cloud in use. Advantages of cloud services are cost-effectiveness, as well as the opportunity to use them, regardless of location, time or device.

The purpose of the study is to determine if the use of the most popular cloud services is threat to users' privacy and data protection. The topic is timely because almost every day there is something about the topic in the news.

The study shows that the largest and the most popular cloud services are reasonably safe to use. For large cloud services these companies can afford to invest in data center security, data security, prevention and service security. The greatest threats to privacy and data protection are the users themselves, because the users can share too much information about themselves.

SISÄLLYS

TERMIT JA NIIDEN MÄÄRITELMÄT

DoS	Denial of Service, palvelunestohyökkäys
IaaS	Infracture as a Service, infrastruktuuri palveluna
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service, sovellusalusta palveluna
SaaS	Software as a Service, ohjelmisto palveluna
SLA	Service Level Agreement, palvelutasosopimus
SOA	Service Oriented Architecture, palvelukeskeinen arkkitehtuuri

1 JOHDANTO

Pilvipalveluiden tarjonta ja niiden käyttäjämäärät ovat viime aikoina kasvaneet nopeasti ja monia sovelluksia ja palveluita markkinoidaan pilviominaisuuksilla. Yksi syy pilvipalveluiden kasvaneeseen suosioon on niiden helppous ja saatavuus erilaisilla laitteilla. Monet pilvipalvelut vaativat toimiakseen vain internet-selaimen, joten niitä voidaan käyttää mihin vuorokauden aikaan tahansa ja mistä päin maailmaa tahansa. Koska varsinainen laskenta tapahtuu konesaleissa, voidaan pilvipalveluita käyttää myös kannettavilla laitteilla, joiden teho on rajattu. Käyttäjä voi olla myös varma, että pilvessä toimivassa sovelluksessa tai palvelussa on aina käytössä uusin mahdollinen versio, sillä pilvipalveluntuottaja huolehtii sovelluksen päivityksestä keskitetysti, eikä käyttäjän tarvitse itse päivittää sovellusta uuteen versioon. Myös palveluntuottajalle on hyötyä siitä, että palvelusta on vain yksi versio olemassa, sillä näin ylläpitokuorma vähenee huomattavasti kun vanhoja versioita ei tarvitse enää tukea.

Käyttäjän kannalta pilvipalvelut tuntuvat houkuttelevilta niiden tarjoamien useiden mahdollisuuksien vuoksi. Käyttäjä voi esimerkiksi tallentaa pilveen tiedostoja, joita voi katsoa helposti eri laitteilla, tai vaikka käyttää kalenteria pilvipalveluna, jolloin kalenteritapahtumiin pääsee käsiksi vaivattomasti riippumatta käyttäjän sijainnista tai laitteesta.

Pilvipalveluiden käyttöön liittyy myös ongelmia, kuten esimerkiksi tietoturva ja yksityisyys, jotka ovat pilvipalveluiden suurimpia haasteita. Yksityisyys ja tietoturva verkkopalveluissa ovat lähes päivittäisiä uutisotsikoita, mikä saattaa aiheuttaa turhaakin negatiivista mielikuvaa pilvipalveluita kohtaan.

Tässä opinnäytetyössä tutkitaan, miten kuluttajille suunnatuissa pilvipalveluissa yksityisyyden suoja toteutuu, sekä mietitään mitä käyttäjä voi tehdä yksityisyytensä eteen näitä palveluita käyttäessään.

Työssä keskitytään tietosuojaan ja yksityisyyteen, ja käydään niihin liittyvää lainsäädäntöä lyhyesti läpi. Lainsäädäntö liittyy hyvin läheisesti käyttäjän yksityisyyteen ja tietosuojaan, mutta se ei kuitenkaan ole tämän opinnäytetyön painopisteistä tärkein.

Työ koostuu seitsemästä luvusta. Luvussa 2 esitellään pilvipalveluiden peruskäsitteet ja pilvilaskentaan liittyvät ominaisuudet. Kolmannessa luvussa käydään läpi pilvilaskentaan liittyviä hyötyjä verrattuna työpöytäsovelluksiin sekä esitellään erilaisia ongelmia, joita liittyy pilvilaskentaan. Neljäs luku keskittyy erilaisiin tietoturvauhkiin pilvilaskennassa. Työn viidennessä luvussa käsitellään identiteettiä ja yksityisyyttä. Kuudennessa luvussa tutkitaan työhän valittujen kuluttajille suunnattujen pilvipalveluiden yksityisyyteen liittyviä kysymyksiä, ja mietitään miten käyttäjä voi parantaa omaa tietoturvaa käyttäessään näitä palveluita. Viimeisessä luvussa kootaan yhteenveto työstä.

2 PILVILASKENNAN PERUSKÄSITTEET

Yleinen tapa on ollut käyttää pilveä kuvaamaan internetiä erilaisissa tietoverkkojen kaaviokuvissa sekä abstrahoimaan monimutkaisia infrastruktuureja, joiden tarkempia yksityiskohtia ei ole saatavilla. Tästä tavasta on lähtöisin termi *pilvilaskenta (cloud computing)*. Pilvilaskenta tarkoittaa siis verkon välityksellä tapahtuvaa tietotekniikan resurssien ja eri teknologioiden käyttöä tavalla, jolla voidaan tuottaa, ulkoistaa, hajauttaa ja tehostaa palveluita.

Pilvilaskennalle on tyypillistä se, että resurssit ovat käytettäessä tarvittaessa virtualisoinnin avulla ja se, että resursseja voidaan ottaa helposti käyttöön esimerkiksi ruuhka-aikoina. Tällöin käyttäjälle tulee mielikuva, että hän käyttää vain yhtä tarkoitukseen varattua resurssia, jolle ei tunnu olevan rajoja. Käyttäjä ei ole myöskään tietoinen siitä, miten pilvipalveluntarjoaja on toteuttanut järjestelmänsä ja millaisia teknisiä ratkaisuja järjestelmässä on käytetty.

Pilvilaskentaan liittyy läheisesti termi *pilvipalvelu (cloud services),* jolla tarkoitetaan pilvessä tarjottavaa palvelua, joka voi olla esimerkiksi laskentakapasiteettia tai valmiita sovelluksia, kuten sähköposti, kalenteri tai asiakkuudenhallintajärjestelmä. Pilvipalvelut ovat toisin sanoen kuluttajille ja yrityksille tuotettuja tuotteita ja palveluja, joita käytetään internetin välityksellä.

Monet yksityisille henkilöille tarkoitetut pilvipalvelut ovat täysin ilmaisia. Ilmaispalveluiden rahoitus tapahtuu mainoksilla, jota erilaiset mainosten tarjoajat yrittävät kohdentaa mahdollisimman tarkasti profiiliin sopiville kuluttajille, jotta mainoksista saadaan mahdollisimman suuri hyötyä. Mainosten kohdentamisessa on suuret riskit käyttäjien yksityisyydelle. Yrityksille tarkoitetut palvelut ovat suurimmaksi osaksi maksullisia, eikä niissä ole mainoksia, mikä vähentää yrityskäyttäjien uhkia yksityisyydelle. Yritykset laativat yleensä tarkoin kirjoitettuja sopimuksia, joilla tietoturvauhat ja muut ongelmat voidaan minimoida.

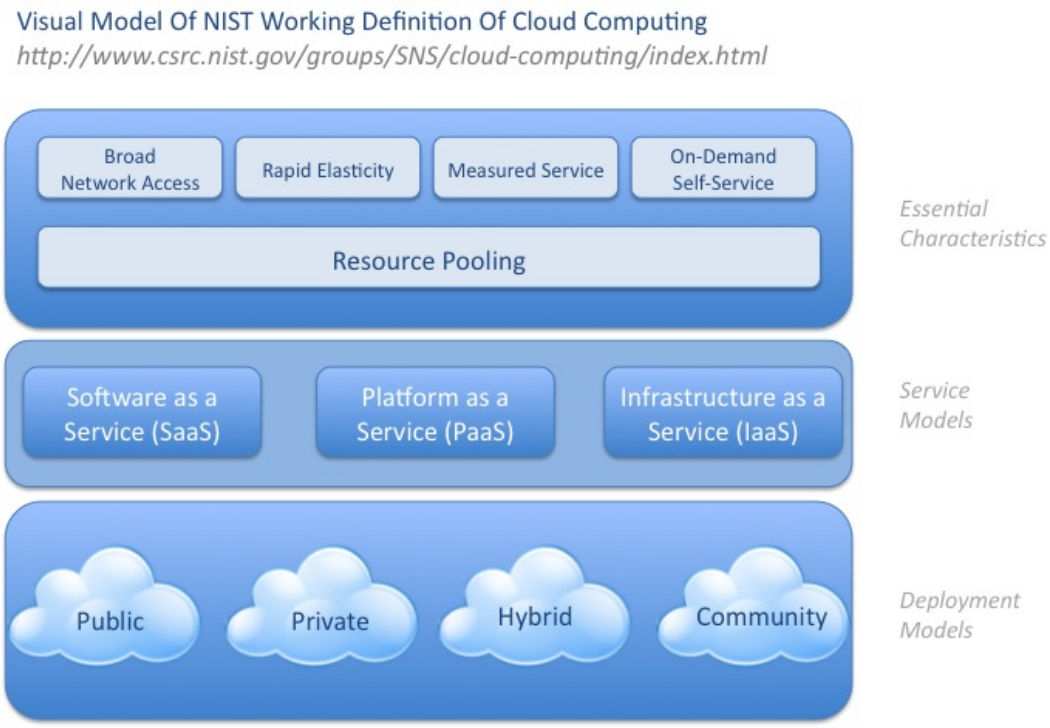
2.1 Pilvipalvelun määritelmä

Koska pilvipalvelu on käsitteenä varsin uusi, sille ei ole vielä yleisesti hyväksyttyä ja laajasti käytettyä määritelmää olemassa. Kirjallisuudessa pilvipalvelu on määritelty monella eri tavalla, mutta useimmiten viitataan NIST:n (National Institute of Standards and Technology) määritelmään vuodelta 2011:

”*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*” [2]

Edellä mainittu määritelmä vapaasti suomentaen:

”Pilvipalvelu on malli, joka mahdollistaa pääsyn verkkoyhteyden yli jaettuihin resursseihin (levytila, sovellukset jne), joita voidaan helposti ottaa käyttöön sekä vapauttaa käytöstä. Pilvipalvelu malli koostuu viidestä ominaispiirteestä, kolmesta palvelumallista ja neljästä käyttöönottomallista.”



Kuva 2.1: Pilvilaskennan määritelmän visuaalinen kuvaus [20]

NIST on Yhdysvaltojen kauppaministeriön alainen virasto, jonka tarkoituksena on kehittää standardeja ja tekniikkaa. NIST:n määritelmässä mainitut pilvilaskennan erityispiirteet ovat käyttö verkon yli, mitattava palvelu, nopea elastisuus, jaetut resurssit ja saatavuus tarvittaessa. Palvelumallit ovat SaaS, PaaS, IaaS ja käyttöönottomallit ovat yksityinen, julkinen, hybridi ja yhteisö. Kuva 2.1 on usein käytetty ja helposti ymmärrettävä visuaalinen malli NIST:n määritelmästä.

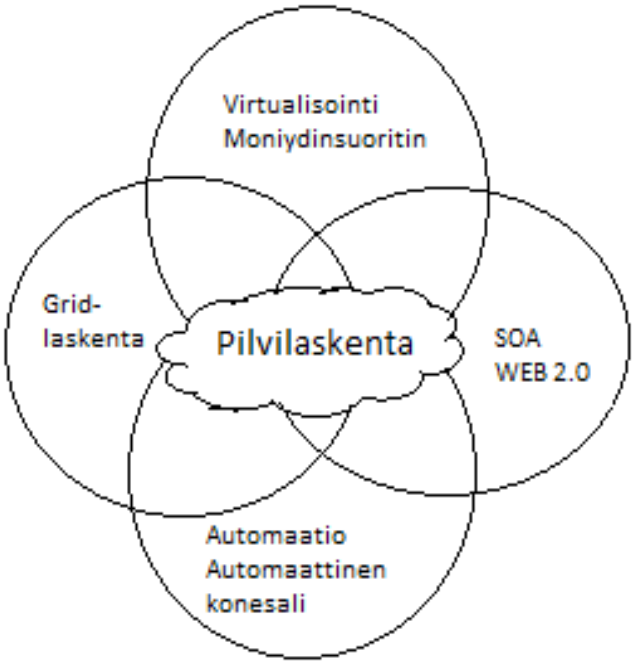
Vaikka määritelmiä löytyy eri lähteistä useita erilaisia, on niissä hyvin usein mainittu seuraavat kohdat:

- **Käyttöperusteinen maksu.** Käyttäjä maksaa vain käyttämistään resursseista.
- **Elastinen kapasiteetti ja loppumattomalta tuntuvat resurssit.** Järjestelmä skaalautuu tarpeen mukaan ilman käyttäjän tietämystä, jolloin käyttäjälle tulee vaikutelma tehokkaasta järjestelmästä, jolle ei tunnu olevan rajoja.

- **Osittainen itsepalvelu.** Käyttäjä voi esimerkiksi itse ottaa palvelun käyttöön heti ilman toimitusaikoja ja käyttäjä voi myös halutessaan muuttaa palvelunominaisuuksia, esimerkiksi lisätä levytilaa, helposti käyttöliittymän kautta.
- **Abstrahoidut tai virtualisoidut resurssit.** Vaikka pilvipalvelu voi toimia ilman virtuaalisia resursseja, on resurssien virtualisointi yleistä sen kustannustehokkuuden vuoksi.

2.2 Pilvilaskennan historia

Pilvilaskenta ei varsinaisesti ole uusi ajatus tai yksittäinen tekninen ratkaisu, vaan sitä voidaan pitää uutena ajattelumallina, jossa tietojenkäsittely ulkoistetaan ja myydään palveluna. Suuret yritykset kuten Google, Yahoo ja Amazon ovat käyttäneet markkinoinnissaan pilvipalvelu-termiä, minkä ansiosta pilvipalvelu on tullut tunnetuksi myös suurelle yleisölle noin viiden viime vuoden aikana.



Kuva 2.2: Pilvilaskenta on monen eri osa-alueen yhdistelmä[3]

Monien eri osa-alueiden kehitys on johtanut pilvilaskennan läpimurtoon. Kuvassa 2.2 havainnollistetaan, miten pilvipalvelu koostuu tai periytyy monesta eri teknologiasta. Pilvilaskennan edeltäjinä voidaan pitää hilalaskentaa, hajautettuja järjestelmiä sekä palvelukeskeistä arkkitehtuuria (SOA, Service Oriented Architecture). Palvelinvirtualisointi ja moniytimiset prosessorit ovat viime vuosikymmenen aikana yleistyneet ja ne ovat nykyään yksi pilvilaskennan peruselementeistä. Samaan aikaan datakeskusten kehitys ja virtualisointi on tuonut lisää automaatiota, jolloin palveluita voidaan tuottaa pienemmällä työmäärällä ja aiempaa edullisemmin. [4]

Viime aikoina myös www-sovelluspalvelut ovat yleistyneet ja kasvattaneet suosiotaan. WWW-sovelluspalveluilla tarkoitetaan www-pohjaisia rajapintoja, joita tarjotaan esimerkiksi HTTP:n yli. Web 2.0 tarkoittaa internetiin liittyvää konseptia, joka kokoaa internetiin liittyviä toimintatapoja. Yhdessä www-sovelluspalveluiden kanssa web 2.0 toimii yhtenä pilvilaskennan osana. [3]

2.3 Pilvilaskennan ominaisuuksia

Koska pilvipalvelu on käsitteenä melko uusi, eri lähteissä määritellään hieman eri lailla pilvipalvelun yleisimmät piirteet. Esimerkiksi NIST[2] käyttää pilvipalvelua määritellessään viittä eri ominaispiirrettä, joita voidaan käyttää aidon pilvipalvelun tunnistamiseen:

- **Käyttö verkon yli.** Jaetut resurssit löytyvät verkkoyhteyden takaa ja resursseja voidaan käyttää tavallisten tietokoneiden tai kannettavien laitteiden avulla. Kaikki laskenta tapahtuu palveluntuottajan päässä, eikä pilvipalvelun käyttämiseen tarvita tehokkaita laitteita.

- **Mitattava palvelu.** Käyttäjää voidaan laskuttaa, kun käyttäjälle tarjottavaa palvelua voidaan mitata. Esimerkiksi voidaan veloittaa käytetystä levytilasta tai vaikka prosessorin käytöstä. Myös sähkönkulutusta voidaan mitata, ja sitä käyttää laskutusperusteena.

- **Saatavuus tarvittaessa ja itsepalvelu.** Käyttäjä voi käyttää pilvipalvelua aina halutessaan riippumatta ajasta tai paikasta. Resurssit ovat aina saatavilla ilman ylläpitäjän apua ja käyttäjä voi esimerkiksi osittain hallinnoida itse palvelua ilman ylläpitäjää.

- **Jaetut resurssit.** Resurssit ovat jaettu käyttäjien kesken ja samalla fyysisellä palvelimella voi toimia samanaikaisesti useita eri palveluita palvelinvirtualisoinnin avulla. Jaetut resurssit ovat yksi syy pilvilaskennan edullisuuteen verrattuna vanhaan malliin, jossa jokaista palvelua kohden oli vähintään yksi fyysinen palvelin.
- **Nopea elastisuus.** Elastisuudella tarkoitetaan pilvilaskennassa sitä, että resursseja voidaan ottaa nopeasti käyttöön kun palvelun kuorma kasvaa ja kuorman laskiessa resursseja voidaan vapauttaa. Käyttäjän kannalta elastisuus tarkoittaa palvelun käyttöönoton helppoutta ja nopeutta. Eli käyttäjä voi ottaa palvelun käyttöönsä nopeasti ja myös irtisanoa palvelun nopeasti.

2.4 Pilven tyyppejä

Pilvipalvelut jaotellaan neljään eri tyyppiin riippuen siitä, että kenellä on oikeus käyttää pilveä ja kenen hallinnassa pilvi on.

2.4.1 Yksityiset pilvet

Yksityiset pilvet sijaitsevat yrityksen omassa tai palvelun tarjoajan konesalissa ja ovat yleensä yrityksen itsensä hallinnoitavissa. Käyttöä voidaan rajata ja valvoa helpommin kuin muissa pilvityypeissä. Koska organisaatio hallinnoi ja valvoo itse pilven resursseja, yksityinen pilvi on pilvityypeistä turvallisin, sillä organisaation ei tarvitse luottaa palveluntarjoajan tarjoamaan tietoturvallisuuteen, vaan voi itse kehittää toimintaansa tukevat ja tarkoituksen sopivat tietoturvakäytännöt. [2]

Vaikka yksityiset pilvet mielletäänkin aina turvallisimmaksi pilvityypiksi, niin todellisuudessa tietoturva voi olla huonompi kuin julkisessa pilvessä. Julkiset pilvet ovat jatkuvasti alttiita hakkerointiyrityksille ja onnistuneet tietoturvamurrot aiheuttavat palveluntarjoajalle negatiivista julkisuutta. Tämä saa palveluntarjoajat pitämään jatkuvaa huolta tietoturvasta ja kehittämään uusia tapoja torjua tietoturvauhkia.

2.4.2 Julkiset pilvet

Julkiset pilven resurssit ovat jaettuja useamman käyttäjän tai organisaation kesken ja resurssit ovat yleensä vapaasti saatavilla julkisen verkon, kuten internetin, yli [2]. Yleensä julkisen pilven omistaa ulkopuolinen palveluntarjoaja, joka voi periä maksua resurssien käytöstä tai rahoittaa toimintaansa mainoksilla. Julkiset pilvet ovat tietoturvaltaan muita pilvityyppejä heikompia, sillä data on talletettu käyttäjän kannalta katsottuna ulkopuolisen palvelimelle. Käyttäjä ei voi olla täysin varma palvelun tarjoaman tietosuojan ja yksityisyyden todellisesta laadusta. Varsinkin pilvipalvelut, joiden toiminta perustuu vain mainoksista saataviin tuloihin, ovat olleet uutisissa erilaisten tietosuojaongelmien vuoksi. [2]

2.4.3 Yhdistelmäpilvet

Yhdistelmäpilvet ovat yksityisen ja julkisen pilven välimuoto. Organisaatio voi esimerkiksi käyttää yksityistä pilveä normaalitilanteissa, mutta kuormituksen äkillisen kasvun aikana voidaan ottaa käyttöön myös julkisen pilven resurssit. [2]

2.4.4 Yhteisöpilvet

Yhteisöpilven käyttäjät voivat olla esimerkiksi yliopistoja, jotka hyödyntävät yhteistä pilveä. Käyttäjiä yhteisöpilvillä on usein vähemmän kuin julkisilla pilvillä, minkä takia yhteisöpilvi tulee kalliimmaksi kuin julkinen pilvi. Tietoturvaltaan yhteisöpilvi on parempi kuin täysin julkinen pilvi, mutta se vaatii organisaatioiden kesken luottamusta. [2]

2.5 Pilvipalveluarkkitehtuurit

Tyypillisimmät pilvipalveluarkkitehtuurit ovat SaaS (Software as a Service), Paas (Platform as a Service) ja Iaas(Infracture as a Serveice). Näiden lisäksi on myös muitakin pilvipalveluarkkitehtuureja, kuten BaaS (Business as a Service) ja MaaS (Management as a Service), jotka ovat ainakin toistaiseksi harvinaisia.

2.5.1 SaaS eli ohjelmisto palveluna (Software as a Service)

SaaS (Software as a Service) on ehkä yksi suosituimmista pilvilaskennan palvelumalleista. Käytännössä SaaS tarkoittaa sitä, että palvelu sijaitsee palveluntarjoajan konesalissa ja palveluntarjoaja on vastuussa asennuksista, ylläpidosta sekä huoltotoimenpiteistä. Asiakas käyttää palvelua esimerkiksi nettiselaimella aina palvelua tarvitessaan. Monet yrityksen tarvitsemat palvelut ovat siirtyneet pilveen ja toimivat SaaS mallin mukaisesti. Esimerkiksi asiakkuudenhallinta-, laskutus-, ja toiminnanohjaussovellukset toimivat usein pilvessä ja niiden välillä voi olla monen tasoisia integraatioita.[4]

Työpöytäsovelluksissa tulee ongelmaksi versioiden päivitys, joka on kallista ja aikaa vievää. Pilvipalvelun käyttäjälle SaaS-ohjelmistot tuovat säästöjä verrattuna työpöytäsovelluksiin, sillä SaaS-ohjelmistoissa ylläpitokustannukset jäävät palveluntarjoajalle, joka voi jakaa kustannukset kaikkien käyttäjien kesken. SaaS-ohjelmistoissa ei yleensä ole myöskään kalliita lisenssimaksuja, sillä hinta määräytyy käytön mukaan.[4]

Kuluttajille SaaS-ohjelmistoja on useita, esimerkiksi Google Apps ja Flickr. Yleensä kuluttajille suunnatut palvelut ovat ilmaisia, mutta palveluntarjoaja rahoittaa toimintaa mainoksilla. Käyttäjän yksityisyyden kannalta mainokset voivat olla ongelmallisia, sillä monet mainostajat yrittävät kohdentaa mainoksia perustuen esimerkiksi käyttäjän hakuhistoriaan. Kuluttajan kannalta SaaS-ohjelmistot ovat houkuttelevia niiden monipuolisten ominaisuuksien ja ilmaisuuden vuoksi.

2.5.2 PaaS eli sovellusalusta palveluna (Platform as a Service)

PaaS eli sovellusalusta palveluna on suunnattu sovelluskehittäjille. Erona SaaS-ohjelmistoihin on se, että käyttäjille ei tarjota valmista sovellusta mitä käyttää, vaan alustan ja ohjelmistorajapinnat joita kehittäjät voivat käyttää. Suurin ongelma PaaS-pilvipalvelussa on rajoittaneisuus, sillä käyttäjällä ei ole täyttä vapautta ohjelmoinnissa vaan käyttäjä kehittää vain järjestelmän osaa kokonaisen järjestelmän sijaan. Hyvänä puolena PaaS-pilvisovelluksissa on skaalautuvuus, josta käyttäjän ei tarvitse huolehtia. [4]

2.5.3 IaaS eli infrastruktuuri palveluna (Infrastructure as a Service)

Iaas eli infrastruktuuri palveluna tarkoittaa sitä, että palveluntarjoaja myy asiakkaalle virtuaalisen konesalin, johon kuuluu esimerkiksi tallennustila, muisti, verkkoyhteys ja laskentateho. Asiakas käyttää virtuaalista konesalia omien palveluiden tuottamiseen. Virtualisoitujen resurssien vuoksi IaaS palvelumalli on edullinen, sillä käytöstä maksetaan vain todellisen tarpeen mukaan ja resursseja voidaan skaalata lisää ruuhkahuippujen aikana automaattisesti. Tämä on suuri hyöty verrattuna itse tuotettuun palveluun, jossa resurssit pitää mitoittaa ruuhkahuippujen tasolle, vaikka suurin osa ajasta palvelun resurssien tarve on vain pieni osa ruuhkahuipusta. [4]

3 PILVILASKENNAN HYÖTYJÄ JA HAASTEITA

Pilvilaskentaan liittyy oleellisia hyötyjä verrattuna työpöytäsovelluksiin. Näiden hyötyjen ansiosta pilvilaskennan suosio kasvaa nopeasti. Samalla pilvilaskentaan liittyy merkittäviä ongelmia, jotka hidastavat pilvipalveluiden yleistymistä. Suurimmat ongelmat liittyvät tietoturvaan, joita käsitellään työn seuraavissa luvuissa.

3.1 Pilvilaskennan hyötyjä

Pilvilaskennassa on useita hyötyjä verrattuna työpöytäsovelluksiin. Tyypillisimmät hyödyt yritykselle tai yksityiselle käyttäjälle ovat seuraavat seikat:

- Ohjelmistojen päivitykset onnistuvat keskitetysti. Tämä helpottaa ohjelmiston ylläpitämistä ja vähentää kustannuksia, sillä ohjelmistosta on vain yksi versio, jota voidaan päivittää keskitetysti. Palvelun käyttäjälle päivitykset eivät välttämättä näy mitenkään, sillä päivitykset voidaan tehdä normaalien toimistoaikojen ulkopuolella. Koska päivitykset eivät vaadi käyttäjältä toimia, asiakasyrityksen it-tuen määrä vähenee mikä saa aikaan säästöjä.
- Pilvisovellukset toimivat myös hitaammillakin laitteilla, sillä varsinainen laskenta tapahtuu palveluntarjoajan päässä.

- Sovellukset ovat käytössä mistä päin maailmaa tahansa internet-selaimella ja yleensä ilman erillisiä lisäosia tai muita asennuksia. Käyttäjän ei siis tarvitse osata esimerkiksi asentaa sovelluksia tai etsiä sovelluksen asennuspaketteja. Joissakin tapauksissa sovellusasennuspaketin mukana on tullut viruksia tai muita haittaohjelmia, vaikka käyttäjä on voinut luulla asentavansa täysin luotettavan ohjelman. Pilvipalveluissa tämä ei ole ongelma, sillä käyttäjän ei tarvitse luottaa ladattuun asennuspakettiin.

- Varmuuskopiointi ei vaadi yleensä käyttäjältä toimenpiteitä, sillä palveluntarjoaja hoitaa varmuuskopioinnit yleensä automaattisesti. Varmuuskopioita tarvitaan mahdollisten laiterikkojen ja inhimillisten erehdysten vuoksi. Usein varmuuskopiointi ei kuitenkaan ole tarjolla ilmaiseksi tuotettuihin kuluttajille suunnattuihin palveluihin vaan niitä tarjotaan yrityksille ja varmuuskopion palauttamisesta otetaan maksu.

- Skaalautuvuus tarpeen mukaan. Ruuhkahuipun aikana otetaan käyttöön enemmän resursseja, jolloin käyttäjät eivät huomaa hitautta ruuhkankaan aikana. Vastaavasti hiljaisempina aikoina ylimääräiset resurssit vapautuvat, ja palvelu toimii vain tarpeen mukaisilla resursseilla.

- Hinnoittelu käytön mukaan. Asiakas saa aikaan säästöjä kun kalliit lisenssimaksut poistuvat ja palvelusta maksetaan vain käytön perusteella. Esimerkiksi jos yritys tuottaa palvelun omassa konesalissaan, joutuu se mitoittamaan laskentatehon tarpeen ruuhkahuipun mukaan. Tällöin hiljaisempina aikoina palvelimet käyvät matalalla kuormituksella mahdollisesti suurimman osan ajasta. Koska palvelu joudutaan mitoittamaan ruuhkahuipun mukaan, kuluu laitehankintoihin ja muihin ylläpitokuluihin rahaa. Kun palvelu tuotetaan pilvipalvelutarjoajan tiloissa, laskentateho skaalautuu oikean tarpeen mukaan ja siten ollen palvelu tulee halvemmaksi kuin sen tuottaminen itse.

Ehkä tärkein ja käyttäjän kannalta mielenkiintoisin pilvilaskennan hyöty on sen riippumattomuus ajasta ja käytettävästä laitteesta. Käyttäjä voi esimerkiksi puhelimella tarkistaa tapahtumat kalenteristaan, johon hän on merkinnyt tapahtumia kotikoneeltaan.

Käyttäjä voi myös hakea asiakkaan tiedot asiakkuudenhallintajärjestelmästä ja pysyä ajan tasalla asiakkuussuhteesta vaikka tien päällä.

Pilvipalveluja kehitetään jatkuvasti ja markkinoille tulee uusia palveluntarjoajia. Onkin oletettavaa, että tulevaisuudessa yhä suurempi osa tietoteknillisestä laskennasta tapahtuu palveluntarjoajan konesalissa ja samalla tarjonnan yleistyessä hintakilpailu kovenee. Käyttäjät voivat hankkia halvalla tai jopa ilmaiseksi lähes kaikki tarvitsemansa sovellukset pilvipalveluna, jolloin päätelaitteeksi kelpaa lähes mikä tahansa laite eikä käyttöjärjestelmälläkään ole väliä. Tulevaisuudessa tietotekniikan siirtyessä yhä enemmän pilveen, tulevat pilvipalveluiden käyttämiseen tarkoitetut laitteet halpenemaan sekä tulemaan vähävirtaisiksi, tarvittavan laskentatehon sijaitessa palveluntarjoajan tiloissa. On mahdollista, että tulevaisuudessa kotitietokoneet jäävät historiaan ja niiden tilalla on vain pieni muistitikun kokoinen laite, jossa on vain internet-selain ja vähän tallennustilaa. Tämä tuo kuitenkin erilaisia ongelmia mukanaan ja niitä käydään läpi tarkemmin seuraavassa luvussa.

3.2 Pilvilaskennan haasteita

Koska pilvipalvelu on vielä melko uusi konsepti, siinä on paljon ongelmia ja haasteita, joita ei ole vielä täysin ratkaistu. Pilvipalvelut myös kehittyvät jatkuvasti, joten uusia ongelmia saattaa ilmetä tulevaisuudessa. Pilvipalveluiden kasvavan suosion vuoksi yhä useammat tahot yrittävät hyötyä tilanteesta laittomin keinoin. Erilaisten huijausten ja haittaohjelmien määrät tulevat kasvamaan samaa tahtia pilvipalveluiden suosion kanssa. Seuraavissa alakappaleissa esitellään tunnetuimpia pilvipalveluiden haasteita ja ongelmia.

3.2.1 Tietoturva ja yksityisyys

Yksi suurimmista haasteista pilvilaskennassa on tietoturva. Varsinkin viime aikoina uutisissa on ollut isoja tietoturvamurtoja, joissa esimerkiksi luottokorttitiedot ovat joutuneet hakkereiden haltuun. Myös salasanoja on vuotanut usein vääriin käsiin. Näistä syistä johtuen kuluttajat ja yritykset ovat alkaneet suhtautuma tietoturvaan entistä vakavammin. [4]

Kuluttajat ovat myös huolissaan yksityisyydestään käyttäessään internetin palveluita. Monet palvelut toimivat mainosrahalla, ja mainostajat yrittävät kohdentaa markkinointia ja mainoksia valituille kuluttajille. Kuluttajien yksityisyys saattaa joutua vaaraan, kun mainostajat pyrkivät saamaan haltuunsa tietoja palveluntarjoajilta. Usein tietoturva perustuu vain luottamukseen palveluntarjoajaa kohtaan, sillä käyttäjällä ei ole mahdollisuutta varmistua toteuttaako palveluntarjoaja riittäviä toimia tietoturvallisuuden ylläpitämiseksi. Tietoturvaa käsitellään tarkemmin luvussa neljä.

3.2.2 Riippuvuus nopeasta internet-yhteydestä

Toinen suuri ongelma pilvipalveluissa on laajakaistan puute suuressa osaa maailmaa. Ilman nopeaa internet-yhteyttä, pilvipalveluiden laatu kärsii ja samalla käyttäjien tuottavuus laskee pitkien latausaikojen takia. Koska pilvipalvelut vaativat toimivan internet-yhteyden, sähkökatkot ja ongelmat internet-yhteyksissä voivat aiheuttaa isoja taloudellisia ongelmia kun pilvipalvelua ei voi käyttää normaalisti. [4]

3.2.3 Epävakaat ohjelmistot

Usein ohjelmistoista löytyy pieniä virheitä, jotka eivät kuitenkaan vaikuta ohjelmiston käytettävyyteen. Välillä ohjelmistoista löytyy vikoja, jotka aiheuttavat suurta vahinkoa. Esimerkiksi vuonna 2011 Microsoftin webpohjainen sähköpostipalvelu Hotmail hävitti useiden käyttäjien sähköpostit[5]. Microsoftin kannalta ongelma ilmeni ikävään aikaan, sillä se oli juuri julkaisemassa Office 365 -pilvipalvelua. Ongelmat sähköpostin kanssa asettavat uuden pilvipalvelun laadun kyseenalaiseksi.

3.2.4 Riippuvuus palvelun tarjoajasta

Jos palveluntarjoaja ajautuu yhtäkkiä konkurssiin, voi olla vaikeaa saada palveluun tallennetut tiedot takaisin omaan haltuun. Tämän takia on hyvä varmistaa ennen palvelun käyttöönottoa, että omien tietojen takaisin saaminen onnistuu helposti jokaisessa tilanteessa.

Myös palvelussa tapahtuvat käyttökatkot saattavat aiheuttaa käyttäjille ongelmia, sillä käyttäjä voi tarvita pilvipalvelua esimerkiksi työnsä suorittamiseen. Joskus käyttökatkot saattavat venyä yllättävän pitkiksi, mikä laskee asiakkaan tuottavuutta ja voivat olla liiketoiminnalle vakavaksi haitaksi. Osaa pilvipalveluista voi kuitenkin käyttää ainakin osittain vaikka internet-yhteyttä ei olisi hetkellisesti saatavillakaan, kun dataa tallennetaan selaimeen muistiin.

Joissakin tapauksissa palveluntarjoaja voi sijaita valtiossa, jonka säädökset ja lait ovat täysin erilaiset mitä käyttäjän kotimaassa. Tällöin ennen pilvipalveluin käyttöönottoa pitää varmistaa, että palveluntarjoajan kanssa tehtävä palvelutasosopimus (SLA, Service Level Agreement) on selkeästä määritelty ja että siinä on määritelty riittävän tarkasti vastuut ja takuut ongelmien ilmetessä.

4 PILVILASKENNAN TIETOTURVAUHKIA

Koska pilvipalvelut toimivat verkkoyhteyden avulla, ne ovat avoinna eri tyyppisille tietoturvauhille. Virukset, madot ja muut haittaohjelmat voivat levitä nopeasti koneesta toiseen ja rikolliset pyrkivät kehittelemään yhä monimutkaisempia haittaohjelmia, joilla yritetään kalastella käyttäjien tietoja tai aiheuttaa muuta vahinkoa. Pilvipalveluihin liittyy myös uusia uhkia, joita ei ole aikaisemmin nähty.

4.1 Tietoturvan määritelmä

Tietoturvalla tarkoitetaan tietojen, ohjelmien, verkkoliikenteen ja palveluiden suojaamista väärinkäytöksiltä. Tietoturva on hyvin tärkeä asia pilvipalveluita käytettäessä. Yleensä tietoturvan määritelmään liittyy kolme kohtaa:

- Luottamuksellisuus eli tietoon pääse käsiksi vain oikeutetut tahot. Ulkopuolisilla ei ole mahdollisuutta käyttää tietoa. Luottamukseen liittyvät ongelmat ovat varsin yleisiä pilvipalveluiden käytössä. Palveluntarjoajan henkilöstöllä on teknisesti mahdollisuus päästä käsiksi asiakkaiden tietoihin. Asiakkaan pitää siis luottaa, että palveluntarjoaja ei ilman lupaa tai hyvää syytä käsittele asiakkaan dataa tarpeettomasti.
- Saatavuus eli kaikki tahot, jolla on oikeus tietoon, pääsee lukemaan tietoa halutessaan eikä ulkopuoliset voi estää tätä. Pilvipalveluissa saatavuus on yleensä

varsin hyvä, monet palvelut lupaavat 99,9% saatavuustason. Suurimmissa pilvipalveluissa datakeskukset ovat hajautettu maantieteellisesti, mikä parantaa saatavuutta.

- Eheys eli tieto on luotettavaa sekä ajan tasalla olevaa. Toisin sanoen, tieto ei ole muuttunut esimerkiksi tahallisesti tai vaikka laitteistovikojen seurauksena.

4.2 Yleisimpiä tietoturvauhkia pilvipalveluissa

Cloud Security Alliance on vuonna 2008 perustettu järjestö, jonka tehtävänä on luoda suosituksia ja käytäntöjä pilvipalveluiden tietoturvallisuuteen ja yksityisyyteen liittyen. Cloud Secure Alliancen suorittamassa tutkimuksessa [6] selvitettiin seitsemän suurinta tietoturvauhkaa pilvipalveluissa. Seuraavissa alaluvuissa käydään läpi tutkimuksessa löytyneet tietoturvauhat.

4.2.1 Pilvipalvelun väärinkäyttö

Pilvipalveluita voidaan väärinkäyttää monella eri tavalla. Cloud Security Alliancen tutkimuksessa[6] havaittiin, että väärinkäyttö liittyy eniten PaaS ja IaaS palvelumalleihin.

Pilvipalvelut ovat yleensä helppo ja nopea ottaa käyttöön ja lisäksi usein on mahdollista ottaa palvelu esimerkiksi kuukaudeksi koekäyttöön. Tällöin on mahdollista, että asiakas voi toimia ainakin osittain tai kokonaan anonyymisti, eikä palveluntarjoajalla ole mahdollisuuksia varmistaa käyttäjän identiteettiä eikä aikeita. Hyökkääjät käyttävät IaaS tai PaaS alustoja muodostamaan bottiverkkoja tai ylläpitämään roskapostipalvelimia. Roskaposti on edelleen suuri ongelma, vaikka sitä onkin saatu viime aikoina karsittua. Sitä vastaan on taisteltu esimerkiksi asettamalla kokonaisia IP-lohkoja estolistalle. [6]

Väärinkäyttöä voidaan vähentää tiukentamalla rekisteröinti- ja validointiprosesseja ja vaatimalla esimerkiksi luottokortin numeron. Samalla pilvipalveluntarjoajan pitää varautua luottokorttihuijauksiin ja toimia yhteistyössä viranomaisten kanssa väärinkäytösten estämiseksi. Tietoliikenteen monitorointi on tärkeässä osassa kun taistellaan väärinkäyttöä vastaan. Liikenteen monitoroinnilla voidaan havaita väärinkäyttö jo aikaisessa vaiheessa, mikä vähentää aiheutuneiden vahinkojen laajuutta. Palveluntarjoajien pitää

jatkuvasti kehittää ja valvoa omia prosessejaan, sillä väärinkäyttäjät pyrkivät koko ajan löytämään uusia keinoja ja aukkoja käyttääkseen pilvipalveluita väärin.

4.2.2 Epäluotettavat rajapinnat

Pilvipalveluiden käyttämiseen ja hallinnointiin vaaditaan erilaisia ohjelmistorajapintoja, kuten SOAP, RESTful, JSON, joiden käyttö tapahtuu yleensä selaimella internetin kautta. Esimerkiksi Twitter ja Facebook tarjoavat ohjelmistorajapintoja, joita ulkopuoliset sovelluskehittäjät voivat hyödyntää omissa ohjelmistoissaan. Pilvipalveluiden käyttäjät käyttävät usein tietämättään näitä rajapintoja. Rajapintoja käytetään esimerkiksi palveluun sisäänkirjautumiseen, monitorointiin ja tiedot välittämiseen. Väärinkäyttö ja virheellisesti toimivat rajapinnat asettavat pilvipalveluiden tietosuojan vaaraan, sillä henkilökohtaiset tiedot voivat päätyä vääriin käsiin. Näistä syistä johtuen, rajapintojen suunnittelussa täytyy varautua ulkopuolisten uhkien minimointiin. Cloud Security Alliance suosittelee salauksen käyttämistä etenkin sisäänkirjautumisessa. [6]

4.2.3 Yrityksen henkilöstö

Yrityksen henkilöstö on yksi suurimmista uhista palvelun tietoturvallisuudelle, sillä henkilöstöllä on pääsy laitetiloihin sekä tietämys palvelun teknisestä toteutuksesta. Yksityisillä käyttäjillä ei ole yleensä mahdollisuuksia saada tietoa palveluntarjoajan käyttämistä rekrytointikriteereistä tai keinoista miten palveluntarjoajan henkilöstöä valvotaan ja pääsyä käyttäjien tietoihin rajoitetaan.

Palveluntarjoajan henkilöstö voi joko vahingossa tai tahallaan aiheuttaa isoja vahinkoja. Henkilöstön aiheuttamia vahinkoja voidaan vähentää rajoittamalla henkilöiden pääsyä kriittisiin paikkoihin. Kulunvalvonnalla voidaan rajoittaa henkilöiden pääsyä fyysisiin paikkoihin. Kulunvalvonnan perusteena on kolmen varmistusmenetelmän käyttö: 1. valtuutus 2. tunnistus 3. kulun- ja yhteydenvalvonta. Valtuutus määrää kuka saa käyttää tiloja tai järjestelmää. Tunnistuksella tarkistetaan henkilön identiteetti. Kulun- ja yhteydenvalvonnalla varmistetaan, että vain valtuutetut henkilöt pääsevät sisään tiloihin tai käyttämään järjestelmään. Vahingoista aiheutuvia haittoja voidaan vähentää myös kouluttamalla yrityksen henkilöstöä säännöllisesti sekä ylläpitämällä selkeitä ohjeita miten pitää toimia eri tilanteissa.

On myös mahdollista, että työntekijä tai henkilö, jolla on pääsy luottamukselliseen tietoon, aiheuttaa täysin tarkoituksella vahinkoa yritykselle. Henkilö voi tahallaan esimerkiksi vaikuttaa palvelun saatavuuteen, tietojen eheyteen tai luottamuksellisuuteen. Henkilö voi myös kopioida yrityksen luottamuksellisia tiedostoja tai lähdekoodeja ja yrittää hyötyä niistä esimerkiksi myymällä tietoja kilpailijalle. Salaamalla luottamukselliset tiedot voidaan vähentää riskiä tietojen päätymisestä vääriin käsiin. [6]

4.2.4 Jaettujen teknologioiden ongelmat

Jaettujen teknologioiden ongelmilla tarkoitetaan infrastruktuurin komponenttien mahdollistamia tietoturvaongelmia. Kaikkia komponentteja (keskussuoritin, välimuistit, näytönohjain...) ei olla suunniteltu tarjoamaan vahvaa tietojen eristämistä multitenanttiarkkitehtuurissa. Virtualisointisovelluksilla voidaan eristää virtualisoidut käyttöjärjestelmät toisistaan. Virtualisointisovelluksissa voi olla vikoja, jotka mahdollistavat pääsyn luvattomiin tietoihin. Jaettujen teknologioiden ongelmat liittyvät vain IaaS palvelumalliin. Koska asiakkaalla on oma virtuaalinen ympäristö, kuten käyttöjärjestelmä, voi asiakas ajaa mitä tahansa ohjelmaa omassa ympäristössään. Hyödyntämällä jaettujen teknologioiden tietoturvaongelmia, asiakas voi päästä joko toisen asiakkaan virtuaaliympäristöön käsiksi tai jollakin tavalla haitata toisen asiakkaan virtuaaliympäristön toimintaa. PaaS ja SaaS pilvipalvelumalleissa asiakkaalla ei ole täyttä kontrollia virtuaaliympäristöön, jolloin jaettujen teknologien ongelmien hyödyntäminen ei onnistu. [6]

4.2.5 Tiedonmenetys ja tietovuoto

Tiedonmenetys voi tapahtua esimerkiksi levyjärjestelmän hajottua tai ohjelman virheen takia ja sillä voi olla suuret vaikutukset asiakkaille. Usein kuitenkin käyttäjä itse aiheuttaa tiedonmenetyksen esimerkiksi poistamalla tiedostoja ja niiden varmuuskopioita. Tieto voidaan menettää myös korruptoitumisen vuoksi tai hakkerin toimesta. Yrityksille suunnatuissa pilvipalveluissa on usein käytössä automaattinen varmuuskopiointi, jolloin kadonneen tiedon palauttaminen on mahdollista. Yksityisille käyttäjille suunnatuissa ilmaisissa pilvipalveluissa ei yleensä ole mahdollisuutta palauttaa varmuuskopioita käyttäjän pyynnöstä, joten käyttäjän kannattaa varmuuskopioida pilveen talletetut tärkeät tiedot omalle koneelle.

Tietovuodolla tarkoitetaan tiedon siirtymistä omistajalta taholle, jolla ei ole tietoon laillisia oikeuksia. Tietovuoto voi tapahtua useilla eri tavoilla, joiden torjuminen on yleensä vaikeaa. Kuten tiedon menetyksessäkin, tietovuoto voi tapahtua käyttäjän itsensä virheestä tai ulkopuolisen toimesta. Käyttäjä voi esimerkiksi lähettää luottamuksellisen sähköpostin väärälle vastaanottajalle, tai jakaa yksityisiä tiedostoja vahingossa muille osapuolille tiedostonjakopilvipalvelussa. Ulkopuolinen tietovuodon aiheuttaja voi olla pilvipalveluntarjoajan työntekijä, joka vahingossa tai tahallaan vuotaa tietoja väärille tahoille. Vahingossa aiheutettuja tietovuotoja voidaan vähentää kouluttamalla ja tiedottamalla tietoturvaa parantavista käytännöistä. Tietovuotoja, jotka tapahtuvat työntekijöiden toimesta, vastaan voidaan suojautua tietojen salaamisella sekä sallimalla käyttäjille pääsy vain sellaisiin paikkoihin, joita käyttäjä tarvitsee työssään. Tällöin vähennetään mahdollisen vuodon koskettamaa tietomäärää. [6]

4.2.6 Käyttäjätilin kaappaus

Hyökkääjät yrittävät hankkia käyttäjätunnuksia ja salasanoja monin eri tavoin. Yleisimpiä tapoja tunnusten kaappaamiseen ovat tietojenkalastelu, virukset ja haittaohjelmat. Tietojenkalastelu tapahtuu yleensä niin, että hyökkääjää lähettää sähköpostia suurelle joukolle. Sähköposti on lähetetty oikean tahon nimissä ja siinä on linkki oikealta näyttävälle sivulle, jossa kysytään esimerkiksi pankin tunnuksia. Usein kalasteluviestit on helppo huomata huonon kieliopin takia. Käyttäjän on myös muistettava, että oikea taho ei kysy koskaan salasanaa tai pankkitunnuksia sähköpostilla.

Pahimmillaan saaduilla käyttäjätunnuksilla ja salasanoilla voidaan kirjautua moneen eri palveluun, mikä lisää tilin kaappauksesta syntyneitä vahinkoja. Käyttäjän kannattaa käyttää eri pilvipalveluissa erilaisia salasanoja, jotka ovat riittävän vahvoja. [6]

4.2.7 Tuntemattomat riskit

Pilvipalveluihin voi liittyä ennalta arvaamattomia riskejä, joihin pilveen siirtyvä yritys ei osaa varautua. Esimerkiksi palveluntarjoajat eivät usein tarjoa tarpeeksi tietoa asiakkaalle, jolloin ongelmiin ei voi varautua. Palveluntarjoajan pitäisi kertoa esimerkiksi datan sijainti, miten riskeihin on varauduttu ja mitä riskejä palvelun käytössä voi olla. Cloud Security Alliance kertoo esimerkkinä tuntemattomista riskeistä tapauksesta, jossa palveluntarjoaja ei ollut paikannut tietoturva-aukkoa vaikka olikin asiasta tietoinen.

4.3 Varautuminen pilven tietoturvauhkiin

John Edwards esittelee Computer Worldin artikkelissaan [15] viisi askelta, joita yrityksen pitäisi käyttää verifioidakseen ja ymmärtääkseen pilvipalvelun tarjoamaa tietoturvaa. Vaikka askeleet ovat tarkoitettu yritysasiakkaille, ne pätevät suurelta osin myös yksityisasiakkaisiin. Nämä viisi askelta ovat:

1. Sen ymmärtäminen, miten pilven uniikki ja avara rakenne vaikuttaa pilveen siirrettyyn dataan. Palvelussa voi olla miljoonia samanaikaisia käyttäjiä, jotka käyttävät samoja rajapintoja ja ainakin osittain samoja resursseja.
2. Läpinäkyvyyden vaatiminen palveluntarjoajalta. Palveluntarjoajalta pitää vaatia tietoa käytetystä tietoturva-arkkitehtuurista sekä mahdollisuudesta auditointeihin, jotka voi suorittaa riippumaton kolmas osapuoli tai valtion tietoturvaviranomainen. Ilman läpinäkyvyyttä on mahdoton sanoa, ovatko tiedot talletettu asian mukaisesti pilveen.
3. Sisäisen tietoturvan vahvistaminen. Palveluntarjoajan sisäisten tietoturvakäytäntöjen ja käytettyjen teknologioiden on oltava hyvällä tasolla, jotta myös pilven tietoturva on kunnossa.
4. Lakien ja säädösten tunteminen. Eri maissa on erilaiset tietosuojakäytännöt, ja ilman tietoturvaa ja -suojaa tukevaa lainsäädäntöä, pilvipalvelun käyttö on riski.
5. Pilvessä tapahtuvien muutosten tarkkailu. Pilvipalvelut kehittyvät jatkuvasti, ja se vaikuttaa myös tietoturvallisuuteen. Tästä syystä on hyvä seurata mitä muutoksia pilviteknologioissa ja käytännöissä tapahtuu, jotta voidaan reagoida ajoissa mahdollisiin ongelmiin. Palvelun käyttöehdot voivat muuttua yllättäen käyttäjälle huonompiin ehtoihin. Tästä on esimerkkinä Instagram, joka ilmoitti joulukuussa 2012 muuttavansa palvelun käyttöehtoja [9]. Muutosten seurauksena Instagram voisi käyttää palveluun ladattuja kuvia mainoksissa. Tämän aiheuttaman kohun vuoksi Instagram kirjoitti käyttöehdot uudelleen, ja samalla se poisti mahdollisuuden käyttää kuvia mainoksissa.

Näitä viittä askelta seuraamalla käyttäjä voi vähentää mahdollisten tietoturvaongelmien uhkaa, mutta askeleet eivät kuitenkaan takaa täydellistä tietoturvaa. Askeleet vaativat myös laajaa tietotekniikan tuntemusta, jota ei kaikilla ihmisillä ole. Esimerkiksi käyttöehdot ovat usein vaikea selkoisia ja niiden ymmärtäminen on vaikeaa etenkin lapsille. Yrityksillä on apuna asianajajat ja tietotekniikkaan perehtyneet asiantuntijat, jolloin ongelmat palvelun laadussa voidaan välttää.

5 YKSITYISYYS JA TIETOSUOJA

Internetissä liikkuu paljon tietoja, joiden on pysyttävä salassa, kuten luottokortin tiedot ja sähköpostikeskustelut. Monet eri tahot voivat olla kiinnostuneita näistä tiedoista ja yrittävät saada niitä haltuunsa. Käyttäjän on hyvä tietää mitä yksityisyydellä ja tietosuojalla tarkoitetaan ja mitkä ovat palveluntarjoajan vastuut käyttäjien tietosuojan ylläpitämisestä. Suomessa lainsäädäntö antaa riittävän tuen turvalliseen verkkokäyttöön, mutta usein tietosuojaongelmia aiheuttavat käyttäjät itse antamalla liikaa tietoja itsestään tai laiminlyömällä tietokoneen tietoturvan, jolloin haittaohjelmat voivat levittää käyttäjän henkilökohtaisia tietoja vääriin käsiin. Pilvipalveluiden käyttöönotto on helppoa, eikä käyttäjän henkilöllisyyttä varmisteta välttämättä ollenkaan. Tämä mahdollistaa identiteettivarkaudet, eli henkilö esiintyy toisena ihmisenä.

5.1 Tietosuoja ja yksityisyys

Tietosuojaan ja yksityisyyteen liittyvistä ongelmista on uutisoitu viime aikoina useasti. Valtionhallinnon tietoturvasanastossa määritellään tietosuoja seuraavasti:

”Ihmisen yksityisyyden suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä. Näitä ovat muun muassa 1) tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen 2) henkilötietojen suojaaminen valtuudettomalta tai henkilöä vahingoittavalta käytöltä.”[10]

Tietosuojalla tarkoitetaan siis yksityisyyden suojaamista ja henkilötietojen käsittelyä. Lainsäädännössä tietosuojaa ja henkilötietojen käsittelyä koskevat sähköisen viestinnän tietosuojalaki sekä henkilötietolaki. Lisäksi perustuslaissa yksityiselämän suoja on määritelty perusoikeudeksi. Yksityisyyteen ja tietosuojaan liittyvä lainsäädäntö käsitellään seuraavassa luvussa.

Yksityiselämän suoja on määrätty Suomen perustuslain 10 §:ssä ja se on jokaiselle kuuluva perusoikeus. Lain mukaan yksityiselämä, kotirauha ja kunnia ovat turvattuja oikeuksia. Perustuslain lisäksi henkilötietolaki, laki yksityisyyden suojasta työelämässä ja sähköisen viestinnän tietosuojalaki sisältävät yksityisyyteen liittyviä kohtia. Yksityisyys on kuitenkin vaikeasti määriteltävissä oleva käsite, sillä se on varsin subjektiivinen käsite. Eri ihmisillä voi olla eri mielipiteet siitä, mitkä asiat kuuluvat yksityisyyteen. Esimerkiksi joku voi pitää poliittista suuntautumisen yksityisenä asiana, kun taas jotkut kertovat julkisesti poliittisen suuntautumisen esimerkiksi sosiaalisessa mediassa. Yksityisyys määritellään Valtionhallinnon tietoturvasanastossa seuraavasti [10]:

1. luonnollisen henkilön oikeus tai käytännön mahdollisuus suojautua ulkopuoliselta puuttumiselta,
2. oikeus tai käytännön mahdollisuus määrätä itseään koskevien henkilötietojen käytöstä,
3. oikeus tulla arvioiduksi oikeiden ja oleellisten henkilötietojen perusteella.

5.2 Lainsäädäntö

Koska pilvipalvelu on käsitteenä varsin uusi, Suomessa ei ole olemassa nimenomaisesti pilvipalveluita koskevaa lainsäädäntöä. Monet olemassa olevat lait koskettavat kuitenkin myös pilvipalveluita, vaikkei lakeja säädettäessä pilvipalveluita ollut vielä olemassa.

Suomessa tietosuojaan ja henkilön yksityisyyteen liittyy useita lakeja ja määräyksiä, joilla pyritään estämään erilaisia väärinkäytöksiä sekä internetissä, että internetin ulkopuolella. Vaikka internet toimii globaalisti, ei ole olemassa ylikansallista lainsäädäntöä koskien pilvipalveluita. Pilvipalveluihin sovellettavia lakeja ovat muun muassa sähköisen viestinnän tietosuojalaki, henkilötietolaki, perustuslaki, laki yksityisyyden suojasta työelämässä ja laki sähköisestä asioinnista viranomaistoiminnassa. Perustuslaissa säädе-

tään oikeus yksityisyydensuojaan. Yksityisyyden suojalla tarkoitetaan sitä, että yksityiselämästä määrääminen on käyttäjän itsensä hallussa.

5.2.1 Perustuslaki

Suomen perustuslain 10 §:n 1 momentin mukaan henkilötietojen suojasta säädetään lailla. Käytännössä tämä tarkoittaa sitä, että perustuslaki antaa lainsäädäntötoimeksiannon. Eduskunnan perustuslakivaliokunta ja hallintovaliokunta ovat määritelleen miten henkilötietojen käsittelystä pitää säätää lain tasolla. Henkilötietojen käsittelyyn liittyviä vaatimuksia ja suosituksia tulee myös kansainvälisistä säädöksistä sekä Euroopan Unionin laeista.

5.2.2 Sähköisen viestinnän tietosuojalaki

Sähköisen viestinnän tietosuojalain tarkoituksena on turvata viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä [11]. Uusi sähköisen viestinnän tietosuojalaki astui voimaan 25.5.2011. Uudessa laissa säädetään, että esimerkiksi evästeitä voidaan tallentaa käyttäjän tietokoneelle vain käyttäjän annettua siihen suostumuksensa. Lisäksi palveluntarjoajan pitää antaa ymmärrettävät ja kattavat tiedot evästeen käytön tarkoituksesta. Käyttäjän kannalta tämä muutos on hyvä asia, sillä evästeitä voidaan käyttää käyttäjän liikkeiden seuraamisessa internetissä. Käyttäjän liikkeitä seuraamalla voidaan esimerkiksi kohdentaa mainontaa juuri käyttäjälle sopivaksi.

5.2.3 Henkilötietolaki

Henkilötietolain tarkoituksena on toteuttaa yksityisyydensuojaa ja yksityisyyttä suojaavia perusoikeuksia henkilötietojen käsittelyssä. Henkilötietolaissa määritellään, että henkilötiedolla tarkoitetaan luonnollista henkilöä tai henkilön ominaisuuksia tai elinolosuhteita kuvaavia merkintöjä, jotka voidaan päätellä henkilöä tai hänen perhettään koskeviksi. Henkilötietojen käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallennusta käyttöä, siirtämistä, luovuttamista, muuttamista ja muita henkilötietoihin kohdistuvia

toimia. Henkilötietolain kolmannessa pykälässä kerrotaan, että henkilötietoja saa käsitellä vain henkilön yksiselitteisesti antamalla luvalla. Laissa taataan oikeus saada selvitys omien tietojen tallentamisesta, eli käyttäjällä on oikeus pyynnöstä nähdä kaikki häntä itseään koskevat tiedot.

Henkilötietolaissa määritellään, milloin tietojen siirtäminen Euroopan unionin ulkopuolelle on sallittua. Lain viidennen luvun yleisissä edellytyksissä säädetään, että tietoja voidaan siirtää Euroopan unionin tai Euroopan talousalueen ulkopuolelle vain, jos kohdemaassa taataan tietosuojan riittävä taso. Yhdysvaltalaisilta yrityksiltä vaaditaan sitoutumista safe harbour -periaatteisiin. [12]

Henkilötietoja voidaan siirtää, jos käyttäjä on antanut yksiselitteisen suostumuksensa siirtoon. Tämän poikkeusperusteen takia käyttäjän kannattaa tutustua huolellisesti pilvipalvelun rekisteriselosteeseen ja muihin käyttöön liittyviin dokumentteihin, jotta käyttäjä ei suostu tietämättään tietojen siirtoon heikon tietosuojan tarjoaviin maihin. [12]

5.2.4 Rikoslaki

Myös rikoslaissa on säädetty pilvipalveluihin sovellettavia säädöksiä, kuten luvussa 38 kerrotaan: ”joka oikeudettomasti 1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka 2) hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai data-siirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta on tuomittava viestintäsalaisuuden loukkauksesta.” Rikoslaissa on määrätty tietomurto ja tietojärjestelmän häirintä rikolliseksi toiminnaksi. Rikoslain luvun 38 pykälä 9 § määrittelee henkilötietojen siirron Euroopan unionin tai Euroopan talousalueen ulkopuolisiin valtioihin henkilötietolain 5 luvun vastaisesti rikolliseksi toiminnaksi. [13]

5.2.5 EU:n tuleva lainsäädäntö

EU-komissio on laatinut ehdotuksen uudeksi tietosuojalainsäädännöksi, jonka tarkoituksena on lisätä Euroopan unionin kansalaisten tietosuojaa ja yhtenäistää lainsäädäntöä. Edellinen tietosuojadirektiivi tuli voimaan 1995, ja se on monilta osin vanhentu-

nut. Uuden tietosuojalain on tarkoitus tulla voimaan vuoden 2014 aikana. Euroopan komissio julkaisi tammikuussa 2012 ehdotuksen uudeksi laiksi [14]. Yhtenä lähtökohdista on ollut yksityisyyden suojan parantaminen rajoittamalla henkilötietojen käsittelyä ja lisäämällä henkilötietojen käsittelyyn liittyviä vaatimuksia. Ehdotuksen mukaan tietosuojaviranomaisille tulisi mahdollisuus sakottaa väärinkäytöistä. Lakiehdotus parantaa käyttäjien mahdollisuuksia poistaa omat tiedostot ja kaiken palveluntarjoajan keräämän datan palvelusta tekemällä tietojen poistamisen mahdollisuuden pakolliseksi. Lakiehdotuksen myötä käyttäjien mahdollisuudet haastaa palveluntarjoaja oikeuteen yksityisyyttä loukkaavista rikkomuksista parantuvat. Lakiehdotus vaikeuttaa kohdennettua mainontaa, sillä tietojen kerääminen ilman lupaa on kiellettyä. Tämä voi vaikuttaa negatiivisesti ilmaisiin palveluihin mainostamisesta saatavien tulojen laskiessa.

Yksi suurimmista muutoksista verrattuna vanhaan lainsäädäntöön on oikeus tulla unohdetuksi, eli käyttäjällä on oikeus pyytää itseään koskevien tietojen poistamista, kun säilyttämiselle ei ole enää perusteltuja syitä. Tämä tekee pilvipalveluiden kokeilemisesta ja käyttämisestä turvallisempaa, koska käyttäjää koskevat tiedot eivät jää palveluun määräämättömäksi ajaksi. Toisaalta jos käyttäjä on julkaisut julkisesti tietoja itsestään, tiedot ovat voineet levitä moniin eri paikkoihin, joista tietojen poistaminen on mahdotonta. Uudesta tietosuojadirektiivistä huolimatta käyttäjän on itse pidettävä huolta tiedoistaan, eikä vain luottaa siihen, että tiedot voitaisiin poistaa kokonaan.

5.3 Uhat yksityisyydelle pilvipalveluissa

Pilvipalveluissa löytyy vakavia uhkia käyttäjien yksityisyydelle ja niiden paikkaaminen on yksi suurimmista pilvipalveluihin liittyvistä haasteista. Käyttäjän henkilökohtaiset tiedot, kuten luottokortin numero, voivat joutua vääriin käsiin. Vaikka käyttäjä pitäisi huolta henkilökohtaisista tiedoista verkossa, voivat ne siltikin vuotaa ulos käyttäjän kontrollista esimerkiksi tietomurtojen tai ohjelmistovirheiden takia. Käyttäjän kannattaa ennen pilvipalvelun käyttöönottoa lukea huolellisesti palvelun tietoturvaselosteet sekä käyttöehdot. Jos palvelun käyttöehdoissa löytyy tietosuojan tai yksityisyyden kannalta ongelmallisia kohtia, kannattaa harkita tarkkaan onko palvelun käyttö niin tarpeellista, että mahdolliset tietoturvauhat voi jättää huomioimatta.

5.3.1 Evästeet ja käyttäjän liikkeiden seuranta

Evästeet (engl. cookie) ovat yleisesti käytössä internetissä. Eväste on pieni tekstimuotoinen tiedosto, jonka palvelin lähettää tietokoneelle. Vaikka evästeet ovat hyödyllisiä ja niitä käytetään suurimmaksi osaksi oikeisiin tarkoituksiin, yhdistetään ne usein käyttäjän liikkeiden seurantaan ja niitä pidetään tietosuojan ja yksityisyyden kannalta ongelmallisina. Sähköisen viestinnän tietosuojalaissa [11] määritellään, että käyttäjälle pitää kertoa evästeiden käytöstä ja käyttäjällä pitää olla mahdollisuus kieltää evästeiden käyttö palvelua käyttäessään. Lain mukaan evästeiden käytöstä ei tarvitse ilmoittaa käyttäjälle, jos käyttäjä on nimenomaisesti pyytänyt kyseistä palvelua tai evästeitä käytetään helpottamaan viestin välittämistä viestintäverkossa tai jos evästeiden käyttö on välttämätöntä palvelun toimimiseksi. On vaikeaa tulkita, että milloin lain tarkoittamat käytön edellytykset toteutuvat. Käyttäjä ei tiedä ovatko evästeet todella tarpeellisia palvelun toiminnan kannalta. Evästeiden käytön rajoja määritellään sähköisen viestinnän tietosuojalain [11] 7.3§:ssä seuraavasti:

Viestintäverkkojen avulla toteutettu evästeiden tai muiden palvelun käyttöä kuvaavien tietojen tallentaminen käyttäjän päätelaitteelle ja näiden tietojen käyttö on sallittua palvelun tarjoajalle, jos palvelun tarjoaja antaa käyttäjälle ymmärrettävät ja kattavat tiedot tallentamisen tai käytön tarkoituksesta. Samalla palvelun käyttäjälle on annettava mahdollisuus kieltää tässä momentissa tarkoitettu tallentaminen tai käyttö.

Edellä 1 momentissa säädetty palvelun tarjoajan tietojen antamisvelvollisuus ja käyttäjän kielto-oikeus ei koske tietojen sellaista tallentamista tai käyttöä, jonka ainoana tarkoituksena on toteuttaa tai helpottaa viestin välittämistä viestintäverkoissa tai joka on välttämätöntä sellaisen palvelun tarjoamiseksi, jota tilaaja tai palvelun käyttäjä on nimenomaisesti pyytänyt. Edellä tässä pykälässä tarkoitettu tallentaminen ja käyttö on sallittua ainoastaan palvelun vaatimassa laajuudessa ja sillä ei saa rajoittaa yksityisyyden suojaa enempää kuin on välttämätöntä.

Evästeet talletetaan käyttäjän koneelle ja yleisesti niiden käyttötarkoituksena on kertoa käyttäjälle, missä osissa sivustoa hän on aikaisemmin käynyt sekä tallentaa sivustoa koskevia asetuksia. Evästeitä käytetään myös tarjoamaan ratkaisu HTTP-protokollan tilattomuuteen. Palvelu tallettaa istunnon ajaksi käyttäjän koneelle evästeen ja se liitetään HTTP-pyyntöjen otsikkotietoihin. Tällöin palvelin pystyy pitämään kirjaa, mihin istuntoon HTTP-pyyntö kuuluu. Evästeitä käytetään yleisesti verkkosivuilla, jotka vaativat

kirjautumista. Eväste voidaan yhdistää luonnolliseen henkilöön kun yhdistellään sisäänkirjautumisen ja palvelun käytön aikana syötettyjä tietoja. [17]

Evästeiden avulla käyttäjän liikkeitä voidaan seurata ja niitä voidaan käyttää apuna mainosten kohdentamisessa. Mainostajat, kuten DoubleClick, asettavat evästeen käyttäjän koneelle kun käyttäjä vierailee sivulla, jossa näytetään DoubleClick-mainoksia. Evästeestä löytyy yksilöllinen evästetunnus, jonka avulla DoubleClick voi päätellä mitkä mainokset käyttäjä on jo nähnyt sekä näyttää käyttäjälle kohdennettuja mainoksia.

DoubleClick kertoo kyseisen menetelmän parantavan mainontaa käyttäjän näkökulmasta, sillä mainoksissa mainostetaan käyttäjää kiinnostavia asioita ja sama mainos ei näy montaa kertaa peräkkäin. Yksi tärkeimmistä mainosten hyödyistä on ilmaisten palveluiden rahoitus. Tietosuojan kannalta kohdistetut mainokset ovat ongelmallisia, sillä tietojen kerääminen tapahtuu käytännössä täysin piilossa käyttäjältä, eikä lupaa tietojen keräämiselle ei kysytä. Tietoja keräämällä DoubleClick saa selville käyttäjän kiinnostuksen kohteet, sekä mahdollisesti iän ja sukupuolen. DoubleClickin käyttöehdoissa kuitenkin kerrotaan, ettei henkilön identifioivia tietoja käytetä mainonnassa. DoubleClick mahdollistaa tietojen keräämisen estämisen käyttämällä uniikin evästetunnuksen tilalla tekstiä ”OPT_OUT”. Tämän voi asettaa myös uusimpien selaimien asetuksista. Vaikka DoubleClick kieltääkin käyttävänsä identifioivia tietoja, on suositeltavaa estää uniikkien evästetunnusten käyttö. Näin käyttäjä voi varmistaa, etteivät mahdolliset muutokset DoubleClickin toiminnassa tulevaisuudessa mahdollista yksilön identifioivia tietojen käyttöä.

Viime aikoina niin kutsutun ”supercookiet” eli superevästeet ovat yleistyneet. Eroina normaaleihin evästeisiin on se, että superevästeiden havaitseminen ja poistaminen on vaikeampaa. Superevästeet toimivat käyttämällä Adoben Flash-tekniikkaa. Flash-mediatoistimen tallentamia tietoja, kuten superevästeitä, ei voi poistaa selaimen avulla vaan käyttäjän täytyy mennä Adoben verkkosivuille poistamaan koneelle tallennetut tiedostot tai käyttäjä voi poistaa superevästeet manuaalisesti, jos superevästeiden hakemistopolku on tiedossa. Jotkut superevästeet pystyvät luomaan normaaleja evästeitä, jolloin ne luodaan uudestaan vaikka käyttäjä poistaisi kaikki evästeet selaimesta. Normaalit evästeet toimivat vain evästeen asettaneella sivulla eikä muut sivustot pysty lukemaan muiden sivustojen asettamia evästeitä. Superevästeet voivat jäljittää käyttäjän liikkeitä usean sivuston kesken, eivätkä ne ole sidottuja selaimeen, mikä tekee käyttäjän seurannasta helppoa.

5.3.2 Tiedon hallinnan menetys

Julkisissa pilvissä kaikki tieto on tallennettu palveluntarjoajan datakeskuksiin, jotka voivat sijaita missä päin maailmaa tahansa. Koska tieto ei ole enää pelkästään käyttäjän hallussa, vaaditaan pilvipalvelun käyttöön luottamusta palveluntarjoajaa kohtaan. Käyttäjä ei tiedä ottaako palveluntarjoaja säännöllisesti varmuuskopioita, tai miten se huolehtii fyysisestä tietoturvasta, puolustautuu tietoturvauhkia vastaan ja korjaa järjestelmässä olevia vikoja, varsinkin kun monet palvelut ovat täysin ilmaisia yksityiskäyttäjille. Vaikka palveluntarjoaja lupaakin pitää tiedot turvassa, niin käyttäjällä ei kuitenkaan ole mahdollisuutta varmistua asiasta läpinäkyvyyden puutteen vuoksi. Myös tietoturva-auditointien pitäminen voi olla mahdotonta tietojen ollessa maantieteellisesti hajautettu. Tiedon hallinnan menetyksestä aiheutuu muun muassa seuraavia ongelmia [7]:

- Käyttäjällä ei ole täyttä varmuutta mitä pilveen tallennetulle tiedolle tapahtuu ja käytetäänkö sitä käyttäjän tietämättä. Jos käyttäjän tieto on julkista, kuten usein yhteisöpalveluissa on, voidaan käyttäjän tietämättä kopioida esimerkiksi kuvia muille sivuille ja niitä voidaan jakaa tai muuttaa.
- Palveluntarjoaja voi täysin tietoisesti käyttää käyttäjien tietoja hyväkseen esimerkiksi kohdistaessaan mainontaa tietyille ryhmille. Sosiaalisen median sovellukset usein kehottavat käyttäjiä jakamaan mahdollisimman paljon tietoa elämästään.
- Mobiililaitteiden pienen tallennustilan ja suorituskyvyn takia osa laitteen sovelluksista voi oikeasti olla pilvisovelluksia käyttäjän tietämättä. Käyttäjälle voi tulla yllätyksenä, että oman tiedon käsitteleminen vaatii internet-yhteyden ja on mahdollista, ettei käyttäjä ole tietoinen sovelluksen tietosuojasta.
- Palvelua käytetään verkon yli, jolloin yhteyttä voidaan salakuunnella tai muuttaa sisältöä. On myös mahdollista estää palveluun pääsy kokonaan palvelunesto-hyökkäyksellä, jolloin käyttäjä ei pääse käsiksi omistamaansa tietoon pilvessä.
- Koska palveluntarjoaja ottaa tiedoista säännöllisesti varmuuskopioita, voi olla mahdotonta poistaa tiedoston jokaista kopiota. Kopio poistetusta tiedostosta voi olla olemassa pitkänkin aikaa.

- Palveluntarjoajan sijaitessa ulkomailla se ei ole Suomen lainsäädännön piirissä, jolloin lait ja määräykset voivat poiketa merkittävästi Suomessa noudatettavista laista ja määräyksistä. Joissakin tapauksissa Suomen lainsäädäntö rajoittaa tiedon siirtoa maahan, jonka tietosuoja ja määräykset ovat heikommat kuin Suomessa[8]. Myös tietoturvallisuuden auditointi on mahdotonta toteuttaa jos palveluntarjoaja sijaitsee ulkomailla.
- Palveluntarjoaja voi pidättää itselleen kaikki oikeudet palveluun talletettavaan tietoon, jolloin palvelun tarjoaja voi esimerkiksi myydä tai välittää tiedot kolmansille osapuolille. Palveluntarjoajat voivat muuttaa yllättäen käyttöehtojaan. Vaikka palvelun tietoturva ja käyttöehdot olisivatkin palvelun käyttöönottohetkellä kunnossa, niin muutokset ehtoihin voivat yllättää käyttäjän.

Riippuvuus pilvipalveluntarjoajasta aiheuttaa käyttäjälle ongelmia, mikäli palveluntarjoaja ajautuu konkurssiin ja palvelu ajetaan alas. Käyttäjä voi varautua mahdollisiin ongelmiin sopimuksilla. Joissakin tapauksissa pilvipalvelut ovat käyttäjälle täysin ilmaisia, eikä ennen käyttöönottoa ole mahdollista tehdä sopimuksia palveluntasosta.

5.3.3 Identiteettivarkaudet

Identiteettivarkaudet ovat yleinen ongelma yksityisyydelle verkossa ja varsinkin yhteisöpalveluissa. Identiteettivarkaudella tarkoitetaan toisen henkilötietojen käyttöä luvatta. Usein väärää identiteettiä käytetään petoksiin, joista tekijä tavoittelee rahallista hyötyä. Esimerkiksi tavaroiden ostaminen ja pikavippien ottaminen toisen nimiin on varsin yleinen teko, niiden tekeminen on kasvussa. Joissakin tapauksessa identiteettivarkauden tavoitteena ei ole rahallinen hyöty, vaan kiusanteko ja mustamaalaus, jotka loukkaavat yksilön yksityisyyttä. Tämänkaltaisia rikoksia tehdään varsinkin sosiaalisessa mediassa, sillä niiden tekeminen on helppoa.

Suomen lainsäädännössä identiteettivarkautta ei ole kielletty. Varkaus on määritelty rikoslain 28 luvun 1 §:ssä ja siinä on määritelty varkauden koskevan irtainta omaisuutta. Henkilön identiteetti ei ole irtainta omaisuutta, joten rikoslaki ei pidä identiteettivarkautta lainvastaisena. Sisäasiainministeriön työryhmän laatimassa raportissa todetaan, että nykyinen lainsäädäntö tarjoaa riittävän suojan identiteettivarkauksien uhreille, sillä varastetun tiedon käyttäminen rikoshyödyn hankkimiseksi on kriminalisoitu. [19]

Suojautuminen identiteettivarkauksilta on vaikeaa, sillä identiteettivarkauteen voi käyttää pelkkää nimeä ja osoitetta, tai vaikka verkossa julkaistua valokuvaa. Käyttäjän kannattaa pitää hyvää huolta kaikkein tärkeimmistä tiedoistaan, kuten luottokortin tiedot ja henkilötunnus, ja ennen niiden luovuttamista varmistua että vastapuoli on luotettava. Käyttäjän on syytä rajoittaa itsestä olevan julkisen tiedon määrää, esimerkiksi piilottamalla ylimääräiset tiedot itsestään sosiaalisessa mediassa kaikilta muilta kuin luotettavilta henkilöiltä.

5.3.4 Muuttuvat ja vaikeasti ymmärrettävät käyttöehdot

Usein pilvipalveluiden käyttöehdot ovat vaikeita ymmärtää. Niiden ymmärtäminen vaatii käyttäjältä hyvää tietoteknistä osaamista ja mahdollisesti myös lakien tuntemista. Ulkomaisten pilvipalveluiden käyttöehdot ovat usein vain englanniksi.

Käyttöehdot muuttuvat usein ja yllättäen, jolloin käyttäjä ei pysty ennalta varautumaan muutoksiin. Monesti käyttöehdot muuttuvat huonompaan suuntaan tietosuojan osalta. Käyttäjä voi varautua näihin uhkiin esimerkiksi etsimällä tietoa palvelusta verkosta. Tiedot ongelmista tietoturvassa ja heikennyksistä käyttöehtoihin päätyvät helposti uutisiin, ja asiasta noussut kohu voi estää palveluntarjoajaa heikentämästä käyttöehtoja. Maksullisissa pilvipalveluissa käyttäjä voi usein solmia tarkemmat käyttöehdot, joiden muuttaminen ei onnistu ilman käyttäjän lupaa.

6 TAPAUSTUTKIMUKSET

Tässä luvussa tehdään tarkempi tutkimus muutaman suosituimman pilvipalvelun tietosuojasta ja millaisia vaikutuksia niillä voi olla käyttäjän yksityisyydelle.

6.1 Linkedin

LinkedIn on jo vuonna 2002 perustettu yhteisöpalvelu, jolla on yli 200 miljoonaa rekisteröitynyttä käyttäjää ympäri maailmaa ja se on maailman suurin ammatilliseen verkostoitumiseen suunnattu palvelu. LinkedIn on tarkoitettu työelämän verkostoitumiseen, ja sen avulla käyttäjät voivat etsiä itselleen työpaikkoja, kertoa omasta osaamisestaan ja työkokemuksestaan luomalla ansioluettelon sekä luoda kontakteja toisiin ihmisiin. LinkedIn on ilmainen, mutta siitä on olemassa myös maksullinen versio. Maksullinen versio tuo enemmän ominaisuuksia, joista on hyötyä etenkin työntekijöitä etsiville. Yritykset etsivät yhä useammin LinkedInin kautta sopivia työntekijöitä korvaten muut rekrytointipalvelut kokonaan.

LinkedInin käyttö on kannattavaa jo opiskelujen aikana. Sen avulla voi etsiä esimerkiksi kesätöitä ja luoda kesätöissä tapaamiinsa ihmisiin yhteyksiä. Yritykset käyttävät yhä useammin sosiaalista mediaa apuna rekrytoinnissa, joten hyvin luotu ja ylläpidetty LinkedIn-profiili helpottaa työn saantia, ja toisaalta puuttuva LinkedIn-profiili saattaa estää joidenkin työpaikkojen saannin.

Koska pilvipalvelun määritelmä on varsin väljä, LinkedIniä voidaan pitää SaaS-pilvipalvelumallin mukaisena pilvipalveluna. LinkedIn täyttää NIST:in määritelmässä olevat viisi kohtaa. Palvelun käyttö tapahtuu verkkoyhteyden avulla ja se on saatavilla tarvittaessa laitteesta riippumatta. Käyttäjä voi myöskin muuttaa palvelun ominaisuuksia, mikä täyttää itsepalvelun merkit. Tietoa siitä, millainen infrastruktuuri LinkedInillä on, ei löydy tarkkaa tietoa. Voidaan kuitenkin olettaa, että palvelussa voidaan ottaa resursseja käyttöön kuormapiikkien aikana. Lisäksi LinkedIn tarjoaa rajapintoja ohjelmistokehittäjille, minkä takia sitä voidaan pitää myös PaaS-palvelumallin mukaisena pilvipalveluna.

LinkedInin käyttöehtojen [21] mukaan käyttäjä omistaa kaiken tiedon mitä palveluun lisätään, mutta LinkedIn pitää täydet oikeudet käyttää kaikkia käyttäjän palveluun lisäämiä tietoja haluamallaan tavalla:

”You grant LinkedIn a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicenseable, fully paid up and royalty-free right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to LinkedIn, including, but not limited to, any user generated content, ideas, concepts, techniques or data to the services, you submit to LinkedIn, without any further consent, notice and/or compensation to you or to any third parties. Any information you submit to us is at your own risk of loss. By providing information to us, you represent and warrant that you are entitled to submit the information and that the information is accurate, not confidential, and not in violation of any contractual restrictions or other third party rights. It is your responsibility to keep your LinkedIn profile information accurate and updated.”.

Käyttöehdoissa kerrotaan myös millä ehdoilla LinkedIn luovuttaa käyttäjän tietoja kolmansille osapuolille:

“*We protect your personal information and will only provide it to third parties: (1) with your consent; (2) where it is necessary to carry out your instructions; (3) as reasonably necessary in order to provide LinkedIn features and functionality to you; (4) as we reasonably believe is permitted by law or regulation; or (5) as necessary to enforce our User Agreement or protect the rights, property, or safety of LinkedIn, its Members, and the public.* ”.

Näiden käyttöehtojen vuoksi käyttäjän täytyy olla hyvin varovainen mitä tietoja lisää palveluun ja lisäksi on varauduttava siihen, että tiedot ovat vapaasti kaikkien saatavilla. Mitään salassa pidettävää tai arkaa tietoa palveluun ei kannata lisätä. Toisaalta esimerkiksi ansioluettelo ja työ- sekä koulutushistoria ovat melko julkista tietoa, esimerkiksi usein työnhaussa joutuu lähettämään ansioluettelon työnantajalle, eikä henkilöllä ole tietoa moniko lukee ansioluettelon ja miten mahdollinen työnantaja säilyttää henkilöiden tietoja.

LinkedIn tarjoaa mahdollisuuden synkronoida osoitekirjan sekä kalenterin mobiililaitteen ja verkkosivun välillä. Kun käyttäjä tekee mobiililaitteella kalenteritapahtuman, niin tapahtuman päivämäärä sekä kaikki osallistujat lisätään LinkedInin omaan kalenterin. Tällöin käyttäjä voi nähdä ketkä kaikki LinkedId-kontaktit ovat osallistumassa tapahtumaan. Vuonna 2012 kalenterin synkronoinnissa olleen ongelman vuoksi kaikki tapahtuman tiedot lähetettiin palvelimelle [22]. Tämä altisti synkronointia käyttävät tahot vakavalle tietovuodolle, sillä usein kalenterikutsuun liittyy salassa pidettävää tietoa. Vaikka LinkedIn kertoo ettei se käytä kalenterikutsuja muuhun kuin yhdistämään osallistujat LinkedIn profiiliin, niin käyttäjällä ei ole mahdollisuutta varmistua asiasta varsinkin kun käyttöehdoissa kerrotaan kaiken tiedon lisäämisen palveluun tapahtuvan omalla riskillä. Tämä on hyvä esimerkki siitä, miten pilvipalvelut tarjoavat erilaisia toimintoja, joista ei ole välttämättä suurta hyötyä, mutta aiheuttavat vakavan uhan käyttäjien yksityisyydelle. Tästä syystä käyttäjän pitää olla hyvin tarkka mitä ominaisuuksia käyttää.

Henkilökohtaisten tietojen lisäksi käyttäjä voi lisätä palveluun myös työnantajaa koskevia tietoja esimerkiksi kuvailemalla menneitä ja nykyisiä työtehtäviä. Tällöin on vaarana paljastaa mahdollisesti luottamuksellisia tietoja työnantajasta, joita kilpailijat voivat hyödyntää. Koska LinkedIn suosittelee käyttäjiään pitämään tietojaan jatkuvasti ajan tasalla, kilpailijoilla on mahdollisuus saada ajankohtaista tietoa yrityksestä. Myös yrityksen asiakkaat voivat seurata yrityksen työntekijöitä LinkedInissä ja saada tietoa esimerkiksi työntekijöistä ja henkilöstössä tapahtuvista muutoksista.

LinkedIn käyttää käyttäjän palveluun syöttämiä tietoja hyväkseen mainonnassa. Käyttäjälle suunnattuja mainoksia näytetään myös LinkedInin ulkopuolella käyttämällä eri mainontaan tarkoitettuja palveluja. LinkedIn käyttää useita eri tapoja käyttäjän seuraamiseen, kuten keksit, IP osoitteet ja ns. web beaconeita, eli pieniä läpinäkyviä kuvia

joiden lataaminen jättää jäljen palvelimelle. LinkedIn kertoo mainosten näyttämisestä ja käytetyistä tavoista seuraavasti:

- *”Advertising technologies like web beacons, pixels, ad tags, cookies, and mobile identifiers as permitted by mobile platforms;*
- *Member-provided profile information and categories (for example, “product managers in Texas”);*
- *Information inferred from a Member’s profile (for example, using job titles to infer age, industry, seniority, and compensation bracket; or names to infer gender).*
- *Your use of LinkedIn (for example, your LinkedIn search history) or clicking on a LinkedIn ad.*
- *Information from advertising partners which we use to help deliver ads more relevant to you* ”

Käyttöehtojen mukaan LinkedIn ei kuitenkaan välitä yksilöivää tietoa kolmansille osapuolille, mutta silti mainostajat saavat varsin tarkan tiedon käyttäjästä ja voivat kohdentaa mainontaa helposti halutuille henkilöille.

LinkedIn on hyödyllinen palvelu kaikille työntekijöille, mutta samalla käyttäjän kannattaa pitää hyvin tarkkaa huolta, siitä mitä hän palveluun lisää. Kohdennettu mainonta, tapahtuneet tietomurrot sekä ongelmat kalenterisynkronoinnin rajapinnoissa on syytä pitää mielessä palvelua käytettäessä. Toisaalta LinkedIn ei käyttöehdoiltaan tai tietoturvauhiltaan eroa muista ilmaisista pilvipalveluista.

6.2 Dropbox

Dropbox on tämän hetken suosituin tiedostojen säilytykseen ja jakamiseen tarkoitettu pilvipalvelu. Dropboxin käyttö on ilmaista, mutta on mahdollista ostaa lisää säilytystilaa. Palvelua voi käyttää esimerkiksi selaimella sekä käyttöjärjestelmään integroituna.

Dropboxin käyttöehdot [23] ovat helppolukuiset, mutta suomenkielinen versio puuttuu. Käyttöehtojen mukaan käyttäjä omistaa kaikki oikeudet palveluun lisäämäänsä tiedostoihin, eikä Dropbox pidätä itselleen minkäänlaisia oikeuksia käyttäjien tiedostoihin.

Tämä poikkeaa useista muista pilvipalveluista, joissa palveluntarjoaja vaatii itselleen oikeuksia kaikkeen käyttäjän lisäämään tietoon. Dropbox ei myöskään jaa käyttäjien tietoja kolmansille osapuolille.

Tietosuojan takaamiseksi myös Yhdysvaltojen ulkopuolella on Dropbox liittynyt Safe Harbor järjestelmään. Poikkeuksena monista muista pilvipalveluista, Dropbox ei näytä ollenkaan mainoksia, joten käyttäjän yksityisyydelle kohdistuu normaalia vähemmän riskejä. Muissa pilvipalveluissa näytetään mainoksia palvelun rahoittamiseen, mutta Dropbox on ns. Freenium markkinointistrategiaa. Ideana on tarjota osa palvelusta ilmaiseksi ja veloittaa tietyistä ominaisuuksista tai tietyiltä käyttäjiltä, esimerkiksi yritysasiakkaat, suurempi levytila tai varmuuskopiointi. Vaikka mainosten puuttumisen takia käyttäjästä kerätyn informaation määrä on pienimpi kuin monissa muissa pilvipalveluissa, kerää Dropbox kuitenkin varsin paljon tietoa käyttäjistä. Käyttäjistä tallennetaan mm. seuraavia tietoja: IP-osoite, käytetyn laitteen tyyppi, sijainti, nimi, puhelinnumero, luottokortin numero, sähköpostiosoite ja kotiosoite. Lisäksi käyttäjä voi tuoda palveluun kontaktitietoja muista palveluista, kuten sähköpostista tai sosiaalisesta mediasta. Kerätyt tiedot ovat kuitenkin varsin yleisesti käytettyjä tietoja ja osittain tarpeellisia palvelun tuottamiseksi eikä Dropbox myy tietoja eteenpäin kolmansille osapuolille.

Monista muista pilvipalveluista eroten, Dropbox julkaisee statistiikkaa viranomaisten pyyntöihin koskien käyttäjien tietoja osoitteessa https://www.dropbox.com/transparency. Tilaistoista selviää ettei Dropbox ole antanut Yhdysvaltojen ulkopuolisille viranomaisille mitään tietoja käyttäjistä. Lisäksi Dropbox vaatii että viranomaispyynnöt tulevat oikeuslaitoksen kautta. Raportti ei kuitenkaan pidä sisällään mahdollisti kansalliseen turvallisuuteen liittyviä pyyntöjä, mikä vähentää tilaston merkitystä. Käyttäjillä ei ole kuitenkaan mahdollisuutta varmistua pitääkö tilastot paikkaansa, sillä mikään ulkopuolinen taho ei valvo tilastoinnin oikeellisuutta.

Dropbox salaa käyttäjien tiedostot käyttämällä AES-256 salausta. Salauksessa tarvittavat avaimet ovat kuitenkin Dropboxin hallussa, eikä käyttäjä pysty asettamaan omaa salausavainta. Ennen kuin tiedosto talletetaan pysyvästi palvelimelle, lasketaan tiedoston tiiviste. Jos joku muu käyttäjä on lisännyt tiivistettä vastaavan tiedoston, ei uutta tiedostoa lisätä palveluun. Toisin sanoen, palvelussa on vain yksi fyysinen kopio tiedostosta vaikka useat käyttäjät olisivat lisänneet saman tiedoston omalle tililleen. Tämä vähentää tallennustilan tarvetta, mutta heikentää tietosuojaa. Koska Dropbox tietää salaukseen käytetyt avaimet, voi Dropboxin työntekijä päästä avaamaan käyttäjien tietoja ilman käyttäjän lupaa. Käyttäjä voi kuitenkin salata tiedostot itse ennen lisäämistä palveluun,

jolloin kukaan ulkopuolinen ei saa tiedostoa auki. Tiedostojen salaamiseen löytyy useita ilmaisia ohjelmia, kuten Boxcryptor, Truecrypt ja GNU PGP. Jos salausohjelma ei tue esimerkiksi mobiilikäyttöjärjestelmiä, niin Dropboxin käytettävyys heikkenee.

Dropbox on melko turvallinen palvelu, eikä sen käyttöön liity yhtä suuria riskejä käyttäjän yksityisyydelle tai tietosuojalla kuin monissa muissa pilvipalveluissa. Varsinkin jos käyttäjä salaa itse tiedostot, niin tärkeiden tietojen vuotaminen ulkopuolisille on epätodennäköistä.

6.3 Oppilaitosten käyttämät pilvipalvelut

Oppilaitokset ovat viime aikoina alkaneet tutkia mahdollisuuksia siirtyä käyttämään pilvipalveluja. Monella oppilaitoksella on oma palvelinkeskus ja henkilökuntaa ylläpitämässä verkkoinfrastruktuuria. Siirtymällä pilvipalveluiden käyttöön, oppilaitos voi säästää merkittävästi kustannuksissa. Esimerkiksi Microsoft ja Google tarjoavat perussovelluksia, kuten sähköpostin ja tekstinkäsittelyohjelmiston, oppilaitoksille ilmaiseksi. Oppilaitoksen ei siis tarvitse enää ostaa lisenssejä käyttämiinsä sovelluksiin eikä verkkopalveluiden ylläpitoon tarvita enää paljoa henkilökuntaa.

Pilvipalveluiden käyttö oppilaitoksissa herättää kysymyksiä, kuten voiko oppilaitos pakottaa oppilaat avaamaan itsellensä Googlen tai Microsoftin tilin? Tai miksi palveluntarjoajat voivat tarjota ohjelmistojaan ilmaiseksi, kun aikaisemmin työpöytäsovelluksista on joutunut maksamaan lisenssimaksuja. Yksi tärkeimmistä asioista on käyttäjien yksityisyys ja tietosuoja. Näiden merkitys on suuri, sillä esimerkiksi yliopistoissa suoritettava tutkimustyö ja siihen liittyvät asiat voivat olla salaisia.

Oppilaan kannalta pilvipalvelut tuovat uusia ja opiskelua helpottavia asioita, kuten reaaliaikainen yhteistyö, tiedoston tallentamisen ja jakamisen ryhmille sekä jaetut kalenterit oppitapahtumien suunnitteluun. Haittana pilvipalveluissa on jatkuvan internet-yhteyden tarvitseminen.

6.3.1 Microsoft Office 365 oppilaitoksille

Microsoft tarjoaa yksityisille, yrityksille sekä oppilaitoksille Office 365 pilvipalvelua, jossa on toimisto-ohjelmat, sähköposti sekä erilaisia työkaluja reaaliaikaiseen kommunikointiin. Oppilaitoksille tarjotaan kolmea erilaista palvelupakettia, joista yksi on ilmainen ja kaksi muuta ovat maksullisia. Ilmaiseksi tarjottava paketti on varsin kattava, se sisältää kaikki oppilaan kannalta tärkeät ominaisuudet kuten sähköposti, tallennustila, kalenteri ja pilvessä toimivat toimisto-ohjelmat. Maksulliset palvelut sisältävät 99,9 % käyttöaikatakuun, eli Microsoft lupaa että 99.9 prosenttia ajasta palvelu on toimintakuntoinen. Lisäksi maksulliset versiot sisältävät lisenssit tietokoneeseen asennettaviin ohjelmistoihin.

Microsoft lupaa kunnioittaa käyttäjän tietosuojaa, eikä se käytä käyttäjien tietoja mainonnan tehostamiseen. Microsoft lupaa myös, ettei se skannaa käyttäjien sähköposteja tai tiedostoja analysointia, mainontaa, tiedonlouhimista tai palvelun parantamista varten. Kaikki palveluun lisätyt tiedot ja tiedostot pysyvät käyttäjän omistuksessa ja käyttäjä säilyttää kaikki oikeudet itselleen. Näiden lupausten ja käyttöehtojen takia palvelun käyttäminen ei aiheuta suurta riskiä käyttäjän tietosuojalle tai yksityisyydelle. Microsoft myöskin kertaa avoimesti missä tiedot sijaitsevat maantieteellisesti. Lisäksi Microsoft on liittynyt Safe Harbor-ohjelmaan.

Koska Office 365 ei sisällä mainoksia, eikä siten kohdennettu mainostaminen ole mahdollista, on sen käyttäminen riittävän turvallista varsinkin oppilaille. Suurimpia uhkia tietosuojalle ovat työntekijät, jotka pääsevät käyttäjien tietoihin käsiksi, sekä Yhdysvaltojen eri viranomaiset, jotka saattavat vaatia pääsyä käyttäjien tietoihin kansalliseen turvallisuuteen vedoten. Ulkopuoliset uhat saattavat olla jopa pienemmät kuin oppilaitosten itsetuottamissa palveluissa, sillä Microsoft pystyy panostamaan tietoturvaan huomattavasti oppilaitosta enemmän.

6.3.2 Google Apps for Education

Google Apps for Education on Googlen pilvipalvelu, joka on suunnattu oppilaitoksille. Tähän palveluun kuuluu sähköposti, kalenteri, tallennustilaa tiedostoille, toimisto-ohjelmat ja videokeskustelut. Lisäksi Googlen sovellukset ovat saatavissa mobiililaitteille, jolloin sovellusten käyttäminen on helpompaa kuin verkkoselaimella. Palvelun käyttäminen on ilmaista, mutta on mahdollista ostaa lisäpalveluita.

Google kertoo, että Google Apps for Education -palvelussa tietoturva ja tietosuoja ovat etusijalla. Esimerkiksi käyttäjä omistaa palveluun lisäämänsä tiedot, eikä Googlella oli niihin oikeuksia. Google on liittynyt Safe Harbor sopimukseen, mikä tarkoittaa että tietosuoja on Euroopan unionin oppilaitoksille asettamien vaatimusten mukainen. Tietoturvallisuuden takaamiseksi palvelu salaa kaiken liikenteen asiakkaan ja palvelimen välillä. Lisäksi on mahdollista käyttää kaksivaiheista tunnistusta, jolloin luvaton tilin käyttö on hyvin vaikeaa. Google Apps for Education on läpäissyt ISAE 3402 Type II tarkistuksen, mikä tarkoittaa sitä, että ulkopuolinen taho on käynyt auditoimassa palvelinkeskusten turvallisuuden. [24]

Google Apps for Educationin suomenkieliset käyttöehdot ovat varsin epäselvät. Niistä käy kuitenkin ilmi, että oppilaitos voi päättää näytetäänkö palvelun käytössä mainoksia. Oletuksina mainosten näyttäminen on estetty, mikä on yksityisyyden kannalta hyvä asia. Mainokset pitää kuitenkin kytkeä päälle entisille opiskelijoille, joiden Google tunnus on vielä voimassa. Oppilaitoksen pääkäyttäjä hallinnoi oppilaitoksen kaikkia tunnuksia. Pääkäyttäjällä on pääsy kaikkeen käyttäjien palveluun lisäämään tietoon, mukaan lukien sähköpostit. Tämä voi olla uhka oppilaiden yksityisyydelle, jos palvelua käytetään muuhun kuin oppimistarkoitukseen. Voidaan ajatella, että kaikki kouluun liittyvä tieto on kuitenkin laadultaan ainakin osittain julkista. Henkilökohtaiseen käyttöön koulun tunnuksia ei kannata käyttää, vaan luoda oma tunnus henkilökohtaisiin tarpeisiin. Google ei jaa käyttäjien tietoja ulkopuolisille. Poikkeuksena on viranomaispyynnöt, joihin Google on pakotettu vastaamaan. Monet Googlea käyttävät oppilaitokset tekevät erikseen sopimuksen palvelun tasosta sekä tietoturvallisuudesta.

6.4 Facebook

Facebook on internetissä toimiva yhteisöpalvelu ja yksi suosituimmista palveluista internetissä. Se on käyttäjälle täysin ilmainen, ja rahoittaa toimintaansa mainostuloilla. Usein käyttäjät eivät kuitenkaan ymmärrä tai tiedosta yksityisyyteen ja tietosuojaan liittyviä ongelmia, joita tulee rekisteröidyttyään palveluun. Facebook kehottaa käyttäjiä jakamaan mahdollisimman paljon tietoa itsestään, jotta Facebook voi käyttää tietoja hyväkseen esimerkiksi mainosten kohdentamisessa. Käyttäjän yksityisyyden kannalta Facebookin kehotus laajasta tietojen jakamisesta on arveluttavaa. Jaettuja tietoja voidaan helposti käyttää väärin ja käyttäjän harkitsemattomasti kirjoitetuista viesteistä voi aiheu-

tua kohu julkisuudessa. Käyttäjän onkin käytettävä harkintaansa ennen kuin julkaisee kirjoituksiaan Facebookissa, sillä kirjoitus voi jäädä internetiin pysyvästi.

Facebook tarjoaa ohjelmistoalustan, jonka avulla ulkopuoliset tahot voivat kehittää sovelluksia. Facebook täyttää siis PaaS-pilvipalvelumallin määritelmän. Facebookia voidaan pitää myös SaaS-pilvipalvelumallina samoilla perusteilla kuin LinkedIniä.

Käyttäjä joutuu itse säätämään Facebookin yksityisyysasetuksia, joita on usein moitittu hankaliksi. Oletuksena Facebook jakaa hyvin paljon tietoja julkisesti, joten yksityisyysasetusten laittaminen kuntoon on järkevää tehdä heti käyttöönoton yhteydessä. Käyttäjällä ei ole mitään tapaa saada selville, että kuka on julkisia tietoja katsellut ja mihin tietoja mahdollisesti käytetään.

Julkisia tietoja voidaan käyttää monella tapaa väärin. Esimerkiksi rikolliset voivat murtautua käyttäjän kotiin sillä aikaa kun käyttäjä on lomamatkalla ja kertoo siitä Facebookissa julkisesti. Onkin suositeltavaa pitää oma profiili mahdollisimman salaisena, ja jakaa tietoa vain tunnettujen henkilöiden, kuten kaverit ja perheenjäsenet, kanssa. Tieto voi päästä vääriin käsiin myös kavereiksi hyväksyttyjen ihmisten kautta, jolloin tiedon leviämisen kontrollointi on vaikeaa. Ohjelmistovirheiden takia luottamuksellisetkin tiedot voivat päättyä julkiseen levitykseen, kuten tapahtui vuonna 2010, jolloin käyttäjien yksityisviestit ja chat-keskustelut oli hetken aikaa mahdollista nähdä käyttämällä hyväksi profiilin esikatselua. Käyttäjä ei voi mitenkään varautua ohjelmistovirheiden aiheuttamiin yksityisten tietojen vuotoihin. Tämän takia on suositeltavaa kirjoittaa Facebookiin vain sellaista tietoa, jota voi paljastaa koko maailmalle ja hoitaa henkilökohtaisemmat asiat turvallisempien kanavien kautta.

Facebookissa on satoja tuhansia sovelluksia, joiden kehittäjänä ovat Facebookin ulkopuoliset tahot. Suuresta määrästä johtuen, kaikkia sovelluksia ei voida tarkistaa Facebookin toimesta, joten mukaan on päässyt useita haittasovelluksia. The Wall Street Journal paljasti vuonna 2010, että useat Facebookin sovellukset olivat jakaneet käyttäjien henkilökohtaisia tietoja mainostajille. Asia kosketti kymmeniä miljoonia ihmisiä, eivätkä edes tiukat yksityisyysasetukset estäneet tietojen päätymistä vääriin käsiin. [18]

Käyttäjän kannattaa säännöllisesti tarkistaa Facebook-tilinsä sovellukset, ja poistaa kaikki sovellukset, joita käyttäjä ei tunnista tai käytä enää. Samalla sovellusten asetuksista kannattaa poistaa lupa käyttää käyttäjän henkilökohtaisia tietoja. Oletusasetukset sallivat sovellusten käyttää lähes kaikkia käyttäjän syöttämiä tietoja hyväkseen. Poista-

malla ylimääräiset sovellukset ja muokkaamalla sovellusten asetuksia käyttäjä voi vähentää mahdollisuuksia omien tietojensa väärinkäyttämiseen.

7 YHTEENVETO

Pilvipalvelut yleistyvät kovaa vauhtia ja yhä useampi käyttäjä käyttää joitakin pilvipalveluita joko oppilaitoksessa tai työpaikassa. Yksi suurimmista syistä pilvipalveluiden kasvavalle suosiolle on niiden tuomat säästöt. Monet pilvipalveluista ovat täysin ilmaisia yksityisille ja yritykselle pilvipalvelut tuovat säästöjä vähentyneiden lisenssimaksujen sekä it-kustannusten vuoksi. Ilmaisuuden haittapuolena on palvelun rahoittaminen mainoksilla. Yritykset pyrkivät saamaan mahdollisimman paljon tuloja mainonnasta ja yksi tehokkaimmista keinoista mainonnan tehostamiseen on mainosten kohdentaminen tarkkaan määritellylle joukolle. Pystyäkseen kohdentamaan mainoksia mahdollisimman hyvin, mainoksia tarjoavat tahot pyrkivät saamaan kaiken mahdollisen tiedon itselleen käyttäjistä. Käyttäjän yksityisyyden kannalta mainosten kohdentaminen on arveluttavaa.

Pilvipalveluihin liittyy useita erilaisia uhkia liittyen käyttäjän yksityisyyteen ja tietosuojaan, joihin liittyvä negatiivinen uutisointi hidastaa pilvipalveluiden suosiota ja kasvuaan. Varsinkin kesällä ilmi tullut vakoiluskandaali on lisännyt käyttäjien negatiivista suhtautumista pilvipalveluihin. Uhkakuvista huolimatta pilvipalveluiden suosio jatkaa kasvua. Suosituimmat pilvipalvelut ovat turvallisia käyttää. Suurimmat uhat yksityisyydelle ja tietosuojalle ovat valtioiden taholta suoritettu vakoilu, tietomurrot sekä käyttäjän omat toimet. Tietomurtoja vastaan käyttäjä voi suojautua käyttämällä vahvoja salasanoja sekä eri salasanaa eri palveluissa. Lisäksi käyttäjä voi salata tiedostot ja sähköpostit, jolloin niiden saaminen auki ulkopuolisen toimesta on vaikeaa. Käyttäjä voi itse aiheuttaa haittaa omalle yksityisyydelleen jakamalla liikaa itsestään tietoja esimerkiksi sosiaalisessa mediassa.

LÄHTEET

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, ja R. Katz, Above the Clouds: A Berkeley View of Cloud Computing, UC Berkeley Reliable Adaptive Distributed Systems Laboratory White Paper, 2009.

[2] P. Mell ja T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Information Technology Laboratory, 2011

[3] R. Buyya, J. Broberg, A. Goscinski, Cloud Computing Principles and Paradigms. John Wiley & Sons, Inc, 2011

[4] J. Rittinghouse, J Ransome, Cloud computing Implementation Management and Security. CRC Press. 2010

[5] K. Thomas, PCWorld. Verkkouutinen 03.01.2011. Viitattu 10.11.2012. Saatavissa http://www.pcworld.com/article/215365/hotmail_data_loss_reveals_cloud_trust_issues.html

[6] Cloud security alliance. Top Threats to Cloud Computing v1.0. 2010

[7] M. Hölbl. Cloud Computing Security and Privacy Issues. The Council of European Professional Information Societies(CEPIS), 2011

[8] Sosiaalisen median tietoturvaohje. Valtiovarainministeriö. 2010

[9] Terms of use. Instagram. Verkkodokumentti. VIitattu.18.12.2012 Saatavissa: http://instagram.com/about/legal/terms/updated/

[10] Valtionhallinnon tietoturvasanasto VAHTI 8/2008. Verkkodokumentti. Viitattu 15-.1.2013. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/name.jsp

[11] Finlex. Sähköisen viestinnän tietosuojalaki.
Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2004/20040516

[12] Finlex. Henkilötietolaki.
Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

[13] Finlex. Rikoslaki.
Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#e-41

[14] Euroopan komissio. Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta. 2012. Saatavissa:
http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_fi.pdf

[15] J. Edwards. Cutting though the fog of cloud security. Verkkodokumentti. Viitattu 3.2.2013. Saatavissa: http://www.computerworld.com/s/article/333530/Cutting_Through_the_Fog_of_Cloud_Security

[16] J. Heiser, M. Nicolett. Assessing the security risks of cloud computing. Gartner 2008.

[17] R. Tirtea, C. Castelluccia, D Ikonomou. Bittersweet cookies. Some security and privacy considerations. Enisa -European Network and Information Security Agency. 2011

[18] E. Steel, G Fowler. Facebook in privacy breach. 2012 Verkkodokumentti. Viitattu 2.3.2013. Saatavissa:
http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html

[19] Sisäasiainministeriö. Henkilöllisyyden luomista koskeva hanke. 2010 Verkkodokumentti. Viitattu 6.8.2013. Saatavissa:
http://www.intermin.fi/julkaisu/322010

[20] Cloudcontrols.org – Cloud assurance compliance. Illustration of Cloud Taxonomy. 2013. Verkkodokumentti. Viitattu 14.8.2013. Saatavissa:
http://www.cloudcontrols.org/cloud-standard-information/cloud-definitions/

[21] LinkedIn privacy policy. Verkkodokumentti. Viitattu 22.08.2013. Saatavissa:
https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv

[22] J. Redfern. More about our mobile calendar feature. LinkedIn blog. 2012 viitattu 3.9.2013. Saatavissa:
http://blog.linkedin.com/2012/06/06/mobile-calendar-feature/

[23] Dropbox Terms of Serrvice. Verkkodokumentti. Viitattu 19.9.2013. Saatavissa:
https://www.dropbox.com/privacy#terms

[24] Google Apps for Education. Verkkodokumentti. Viitattu 26.9.2013. Saatavissa:
http://www.google.com/intx/fi/enterprise/apps/education/benefits.html#together